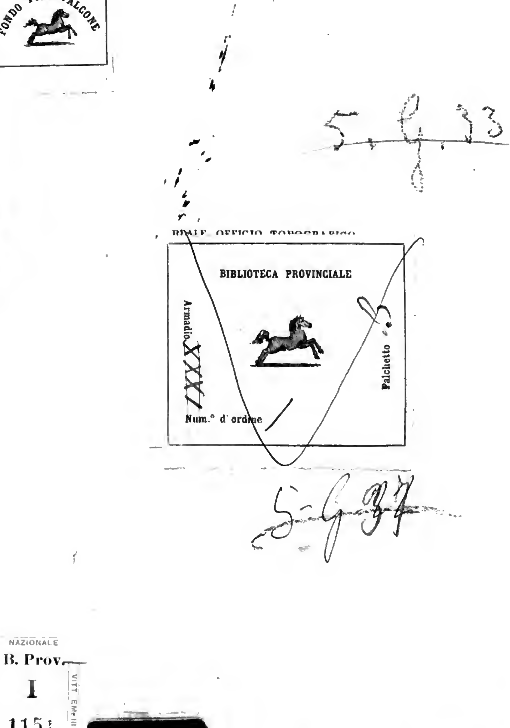
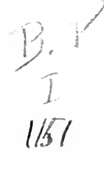
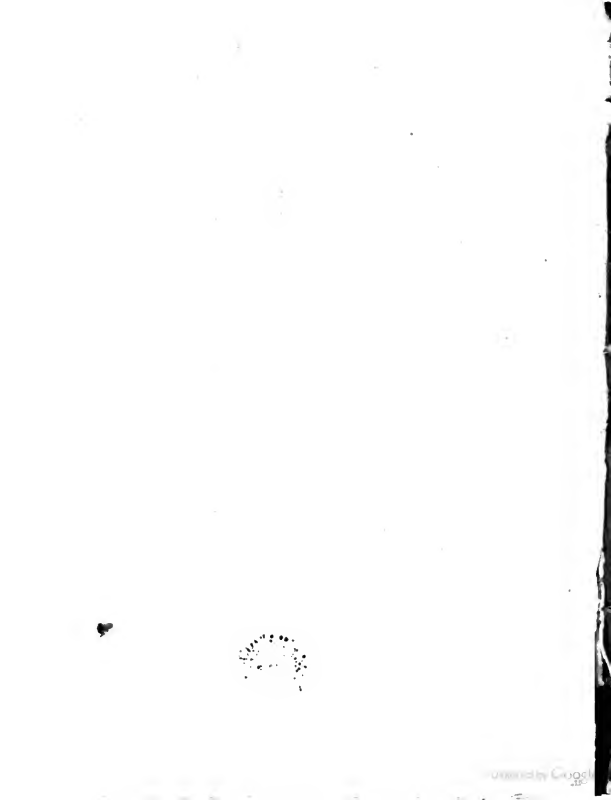



FONDO PIZZOFALCONE
5. G. 33
REALE OFFICIO TOPOGRAFICO
BIBLIOTECA PROVINCIALE
Armadio XXXX
Palchetto
Num.° d' ordine
5-G-37


B. I
1151



# ESSAI

# SUR LA THÉORIE

# DES NOMBRES;

Par A. M. LE GENDRE, de l'Institut national.

A PARIS,

Chez DUPRAT, Libraire pour les Mathématiques, quai des Augustins.

AN VI.





# PRÉFACE.

A EN juger par différens fragmens qui nous restent, et dont quelques-uns sont consignés dans Euclide, il paroit que les anciens Philosophes avoient fait des recherches assez étendues sur les propriétés des nombres. Mais il leur manquoit deux instrumens pour approfondir cette science, l'Art de la numération qui sert à exprimer les nombres avec beaucoup de facilité, et l'Algèbre, qui généralise les résultats, et qui peut opérer également sur les connues et les inconnues. L'invention de l'un et l'autre de ces arts dut donc influer beaucoup sur les progrès de la science des nombres. Aussi voit-on que l'ouvrage de Diophante d'Alexandrie, le plus ancien Auteur d'algèbre qu'on connoisse, est entièrement consacré aux nombres, et renferme des questions difficiles résolues avec beaucoup d'adresse et de sagacité.

Depuis Diophante jusqu'au temps de Viete et de Bachet, les Mathématiciens continuèrent de s'occuper des nombres, mais sans beaucoup de succès, et sans faire avancer sensiblement la science.

Viete, en ajoutant de nouveaux degrés de perfection à l'Algèbre, résolut plusieurs problèmes difficiles sur les nombres. Bachet, dans son ouvrage intitulé *Problèmes plaisans et délectables*, résolut l'équation indéterminée du premier degré par une méthode générale et fort ingénieuse. On doit à ce même Savant un excellent commentaire sur Diophante, qui fut depuis enrichi des notes marginales de Fermat.

Fermat, l'un des Géomètres dont les travaux contribuèrent le plus à accélérer la découverte des nouveaux calculs, cultiva avec un grand succès la science des nombres, et s'y

fraya des routes nouvelles. On a de lui un grand nombre de Théorêmes intéressans, mais il les a laissés presque tous sans démonstration. C'étoit l'esprit du temps de se proposer des problêmes les uns aux autres. On cachoit le plus souvent sa méthode, afin de se réserver des triomphes nouveaux tant pour soi que pour sa nation; car il y avoit sur-tout rivalité entre les Géomètres françois et les anglois. De-là il est arrivé que la plupart des démonstrations de Fermat ont été perdues, et le peu qui nous en reste, nous fait regretter d'autant plus celles qui nous manquent.

Depuis Fermat jusqu'à Euler, les Géomètres, livrés entièrement à la découverte ou à l'application des nouveaux calculs, ne s'occupèrent point de la Théorie des Nombres. Euler, le premier, s'attacha à cette partie; les nombreux Mémoires qu'il a publiés sur cette matière dans les Commentaires de Pétersbourg, et dans d'autres ouvrages, prouvent combien il avoit à cœur de faire faire à la science des Nombres les mêmes progrès dont la plupart des autres parties des Mathématiques lui étoient redevables. Il est à croire aussi qu'Euler avoit un goût particulier pour ce genre de recherches, et qu'il s'y livroit avec une sorte de passion, comme il arrive à presque tous ceux qui s'en occupent. Quoi qu'il en soit, ses savantes recherches le conduisirent à démontrer deux des principaux Théorêmes de Fermat, savoir 1°. que si $a$ est un nombre premier, et $x$ un nombre quelconque non divisible par $a$, la formule $x^{a-1}-1$ est toujours divisible par $a$; 2°. que tout nombre premier de forme $4n+1$, est la somme de deux quarrés.

Une multitude d'autres découvertes importantes se font remarquer dans les Mémoires d'Euler. On y trouve la théorie des diviseurs de la quantité $a^n \pm b^n$, le traité *de partitione nume-*

*rorum*, qui est inséré aussi dans son *Introd. in Anal. inf.*, l'usage des facteurs imaginaires ou irrationnels dans la résolution des équations indéterminées, la résolution générale des équations indéterminées du second degré, en supposant qu'on en connoisse une solution particulière ; la démonstration de beaucoup de Théorèmes sur les puissances des nombres, et particulièrement de ces propositions négatives avancées par Fermat, que la somme ou la différence de deux cubes ne peut être un cube, et que la somme ou la différence de deux biquarrés ne peut être un quarré. Enfin on trouve dans ces mêmes écrits un grand nombre de questions indéterminées résolues par des artifices analytiques très-ingénieux.

Euler a été pendant long-temps presque le seul Géomètre qui se soit occupé de la Théorie des Nombres. Enfin la Grange est entré aussi dans la même carrière, et ses premiers pas ont été signalés par des succès égaux à ceux qu'il avoit déjà obtenus dans des recherches d'un genre plus sublime. Une méthode générale pour résoudre les équations indéterminées du second degré, et, ce qui étoit plus difficile, une méthode pour les résoudre en nombres entiers, fut le coup d'essai de ce Savant illustre ; bientôt après il appliqua les fractions continues à cette branche d'analyse ; il démontra le premier que la fraction continue égale à la racine d'une équation rationnelle du second degré, devoit être périodique, et il en conclut que le problême de Fermat concernant l'équation $x^2-Ay^2=1$, est toujours résoluble ; proposition qui n'avoit pas encore été établie d'une manière rigoureuse, quoique plusieurs Géomètres eussent donné des méthodes pour la résolution de cette équation.

Le même Savant, par des recherches ultérieures qui sont consignées dans les Mémoires de Berlin, a démontré le pre-

mier que tout nombre entier est la somme de quatre quarrés; on lui doit également plusieurs autres démonstrations importantes, mais la plus remarquable de ses découvertes est une méthode générale de laquelle découlent comme corollaires une infinité de Théorêmes sur les nombres premiers.

Cette méthode, singulièrement féconde, est fondée sur la considération des formes tant quadratiques que linéaires qui conviennent aux diviseurs de la formule $t^2 + au^2$, où $t$ et $u$ sont deux indéterminées, et $a$ un nombre donné. Il restoit cependant à établir, d'une manière générale, la relation qui doit exister entre les formes linéaires et les formes quadratiques appliquées aux nombres premiers; car au défaut du principe qui contient cette relation (1), la Théorie de la Grange, qui donne une infinité de Théorêmes pour les nombres premiers $4n-1$, n'en fournit qu'un très-petit nombre relatifs aux nombres premiers $4n+1$.

Un Mémoire que j'ai publié dans le volume de l'Académie des Sciences pour l'année 1785, offre les moyens de démontrer le principe dont il s'agit, et renferme d'ailleurs des propositions qui paroissent avancer la science des nombres. J'y ai donné 1°. la démonstration d'un Théorême pour juger de la possibilité ou de l'impossibilité de toute équation indéterminée du second degré, ramenée à la forme $ax^2 + by^2 = cz^2$; 2°. la démonstration d'une loi générale qui existe entre deux nombres premiers quelconques, et qu'on peut appeler *loi de réciprocité;* 3°. l'application de cette loi à diverses propositions, et son usage, tant pour perfectionner la Théorie de la Grange, que pour vaincre d'autres difficultés du même genre.

(1) Voyez sur cet objet les Mémoires de l'Académie des Sciences de Berlin, année 1775, pag. 350 et 352.

Le

Le même Mémoire contient en outre l'ébauche d'une théorie entièrement nouvelle sur les nombres considérés en tant qu'ils sont décomposables en trois quarrés; théorie à laquelle appartient le fameux Théorême de Fermat, qu'un nombre quelconque est la somme de trois triangulaires, et cet autre Théorême du même Auteur, que tout nombre premier $8n-1$ est de la forme $p^2+q^2+2r^2$.

Depuis l'époque de la publication de ce Mémoire, je me suis occupé à diverses reprises de développer les vues qu'il contient, et d'apporter quelques perfectionnemens à différens points de la Théorie des Nombres et de l'analyse indéterminée (1). Mes recherches à cet égard ayant été suivies de quelque succès, je me proposois d'abord d'en publier le résultat dans un ouvrage particulier; j'ai cru ensuite devoir profiter de cette occasion pour traiter la Théorie des Nombres avec plus d'étendue qu'on ne l'a fait jusqu'à présent (2), et en y comprenant le résultat des principales recherches d'Euler et de la Grange sur la même matière.

C'est ainsi que je me suis déterminé à composer l'ouvrage que j'offre en ce moment au Public; je le donne non comme

(1) Je ne sépare point la théorie des nombres de l'analyse indéterminée, et je regarde ces deux parties comme ne faisant qu'une seule et même branche de l'analyse algébrique. En effet, il n'est pas de Théorême sur les nombres qui ne soit relatif à la résolution d'une ou de plusieurs équations indéterminées. Ainsi quand on assure, d'après Fermat, que tout nombre premier $4n+1$ est la somme de deux quarrés, c'est comme si on disoit que l'équation $A=y^2+z^2$ est toujours résoluble tant que $A$ est un nombre premier de forme $4n+1$. On peut ajouter que dans ce même cas l'équation $A=y^2+z^2$ n'aura jamais qu'une solution, ce qui est un second théorême contenant une propriété caractéristique des nombres premiers $4n+1$.

(2) Le traité d'analyse indéterminée faisant suite à l'Algèbre d'Euler, et enrichi des additions de la Grange, est sans doute un ouvrage excellent en ce genre, mais il ne contient guère que la partie élémentaire.

un traité complet, mais simplement comme un essai qui fera connoître à-peu-près l'état actuel de la science, et qui contribuera peut-être à en accélérer les progrès. Il ne m'appartient pas d'en dire davantage sur mon propre ouvrage; j'ajouterai seulement que je n'ai rien négligé pour le rendre digne de l'attention des Géomètres. Mais quelque soin que j'aie mis à examiner les divers cas particuliers de plusieurs propositions, je sens qu'il a pu m'échapper des omissions et peut-être même des erreurs. Je ne doute pas sur-tout que plusieurs des propositions nouvelles que j'ai démontrées laborieusement, ne le puissent être d'une manière beaucoup plus simple, soit à l'aide de principes encore inconnus, soit par des rapprochemens que je n'ai pas apperçus. Quoi qu'il en soit, j'ose me flatter qu'à raison de la difficulté de la matière et de sa nouveauté, les Géomètres recevront ces essais avec indulgence, et j'espère que les fautes même dans lesquelles j'aurois pu tomber, tourneront au profit de la science, en donnant occasion à des mains plus habiles de traiter le même sujet, et de le porter à un plus haut degré de perfection.

# TABLE DES MATIÈRES.

## INTRODUCTION,

*Contenant des notions générales sur les Nombres.*

On considère les nombres en tant qu'ils résultent de la multiplication de plusieurs facteurs, pages 1—8
Diverses propositions sur les nombres premiers, 8—12
On cherche combien il y a de nombres premiers dans $n$ termes consécutifs d'une suite à différences égales, 15
Table nécessaire pour cette détermination, 17
Table des nombres premiers de 1 à 1000, 20

## PREMIÈRE PARTIE.

*EXPOSITION DE DIVERSES MÉTHODES ET PROPOSITIONS RELATIVES A L'ANALYSE INDÉTERMINÉE.*

§. I. *Des fractions continues*, 21
Définition des quotiens-complets, et des fractions convergentes, 22—24
Propriétés générales des fractions convergentes, 24—27
Condition pour qu'une fraction donnée soit comprise parmi les fractions convergentes, 28
Application à l'équation $p^2-Aq^2=\pm D$, 29
Des fractions continues symmétriques, 31
§. II. *Résolution des équations indéterminées du premier degré*, 32
§. III. *Méthode pour résoudre en nombres rationnels les équations indéterminées du second degré*, 35
Réduction de l'équation générale à la forme $x^2-By^2=Az^2$, 36
Résolution de l'équation $x^2-y^2=Az^2$, 37
On donne, d'après la Grange, les moyens de diminuer successivement les coefficiens $A$ et $B$, jusqu'à ce que l'un d'eux soit égal à l'unité, 38—42
§. IV. *Théorême pour juger de la possibilité ou de l'impossibilité de toute équation indéterminée du second degré*, 43
On démontre que l'équation $ax^2+by^2=cz^2$ est possible, si l'on peut trouver

trois entiers $\lambda$, $\mu$, $\nu$ tels que les trois quantités $\frac{a\lambda^2+b}{c}$, $\frac{c\mu^2-b}{a}$, $\frac{c\nu^2-a}{b}$ soient des entiers. Autrement elle sera impossible, 49

§. V. *Développement de la racine d'un nombre non quarré en fraction continue*, 50

Loi générale du développement, 53

On prouve que la fraction continue est périodique, 54

On en conclut que l'équation $x^2 - Ay^2 = 1$ admet toujours une infinité de solutions, 57

§. VI. *Résolution en nombres entiers de l'équation* $x^2 - Ay^2 = \pm D$, *D étant* $< \sqrt{A}$, 58

Condition pour que l'équation soit possible, 61

Formules générales qui contiennent une infinité de solutions de l'équation proposée, 63

§. VII. *Théorêmes sur la possibilité de l'équation* $x^2 - ay^2 = -1$, *2 ou* $-2$, *a étant un nombre premier*, 65

L'équation $x^2 - ay^2 = -1$ sera possible, si $a$ est un nombre premier $4n+1$, *ibid.*

L'équation $x^2 - ay^2 = -2$ sera possible, si $a$ est un nombre premier $8n+3$, 66

L'équation $x^2 - ay^2 = 2$ sera possible, si $a$ est un nombre premier $8n-1$, 67

§. VIII. *Réduction de la formule* $Ly^2 + Myz + Nz^2$ *à l'expression la plus simple*, 69

On suit pour cette réduction la méthode donnée par la Grange dans les Mémoires de Berlin, année 1773. On démontre, par une méthode particulière, que deux formules $py^2 + 2qyz + rz^2$, $p'y^2 + 2q'yz + r'z^2$, dans lesquelles $pr - q^2$ et $p'r' - q'^2$ sont égales à un même nombre positif $A$, sont différentes l'une de l'autre, si d'ailleurs elles sont préparées de manière que le coefficient moyen ne surpasse aucun des extrêmes, 75

§. IX. *Développement de la racine d'une équation du second degré en fraction continue*, 77

Loi générale du développement, la même que pour les simples racines quarrées, 79

On prouve que la fraction continue est périodique, 80

On détermine l'expression générale des diverses fractions convergentes qui répondent à un même quotient dans les périodes successives, 82

Observations sur la résolution de l'équation $fy^2 + gyz + hz^2 = \pm D$, 86

§. X. *Comparaison des fractions continues résultantes du développement des deux racines d'une même équation du second degré*, 90

On prouve que la période comprise dans le développement d'une racine est l'inverse de la période comprise dans le développement de l'autre racine.

§. XI. *Résolution en nombres entiers de l'équation* $Ly^2+Myz+Nz^2=\pm H$, 99

Il ne peut y avoir une infinité de solutions que lorsque $M^2-4LN$ est un nombre positif non quarré; on résout alors l'équation en la ramenant au cas où le second membre $=\pm 1$, 103

On confirme par divers exemples la remarque déjà faite, que les formules obtenues par le développement d'une racine contiennent implicitement le résultat du développement des deux racines, 110

§. XII. *Démonstration d'une proposition supposée dans les paragraphes précédens*, 115

Étant proposée l'équation $fy^2+gyz+hz^2=\pm H$, dans laquelle $H$ est $<\frac{1}{2}\sqrt{(g^2-4fh)}$; si cette équation est résoluble, la fraction $\frac{y}{z}$ doit se trouver parmi les fractions convergentes vers une racine de l'équation $fx^2+gx+h=0$, 115—120

Les cas, qui semblent faire exception, sont néanmoins compris dans les formules générales, 121

§. XIII. *Réduction ultérieure des formules* $Ly^2+Myz+Nz^2$ *lorsque* $M^2-4LN$ *est égal à un nombre positif*, 123

On donne pour cet objet une méthode directe fondée sur le développement en fraction continue d'une racine de l'équation $Lx^2+Mx+N=0$, 126

Les Tables I et II sont construites en conséquence de cette théorie, elles offrent les réductions toutes faites pour un grand nombre de formules. *Voyez le recueil des Tables.*

§. XIV. *Développement en fraction continue des racines des équations d'un degré quelconque*, 133

Méthode générale due à la Grange. — Perfectionnement ajouté à cette méthode par le même Auteur, 136

Observation sur le nombre des quotiens nouveaux qu'on peut déduire des quotiens déjà trouvés, 139

Exemples de développemens qui offrent des rapports remarquables entre les racines, 143

Observations sur la solution de quelques équations indéterminées d'un degré élevé, 147

Rapport remarquable entre les racines des transformées successives et les racines de la proposée, 152

Développement d'une racine réelle de toute équation proposée, 157

Méthode pour obtenir la première approximation dans les équations algébriques, 159

Approximation pour les racines imaginaires, 161

§. XV. *Résolution en nombres entiers de l'équation indéterminée* $Ly^n + My^{n-1}z + Ny^{n-2}z^2 \ldots + Vz^n = \pm H$, 169

On ramène cette équation au cas où le second membre $= \pm 1$, *ibid.*

Recherche sur les moyens de déterminer $y$ et $z$ pour que la fonction homogène $at^n + bt^{n-1}u + ct^{n-2}u^2 \ldots + ku^n$ soit un *minimum*, 170

On prouve que dans le cas du *minimum* la fraction $\frac{t}{u}$ doit être l'une des fractions convergentes vers une racine réelle de l'équation $ax^n + bx^{n-1} + \ldots + k = 0$, ou vers la partie réelle d'une racine imaginaire de cette même équation, 175

## SECONDE PARTIE.

### *PROPRIÉTÉS GÉNÉRALES DES NOMBRES.*

§. I. *Théorêmes sur les nombres premiers*, 181

On démontre que si $c$ est un nombre premier, et $N$ un nombre quelconque non divisible par $c$, la quantité $N^{c-1} - 1$ sera divisible par $c$, *ibid.*

Si $n$ est un nombre premier, le produit $1 . 2 . 3 \ldots (n-1)$ augmenté de l'unité, sera divisible par $n$, 182

Si $c$ est un nombre premier, et $P$ un polynome en $x$ du degré $m$, il ne pourra y avoir plus de $m$ valeurs de $x$ comprises entre $-\frac{1}{2}c$ et $+\frac{1}{2}c$, qui rendront $P$ divisible par $c$, 184

Si un polynome du degré $m$ divise $x^{c-1} - 1$ ou $x^{c-1} - 1 + cR$, il y aura toujours $m$ valeurs de $x$ qui rendront ce polynome divisible par $c$, 185

Le nombre premier $c$ sera diviseur de $x^2 + N$, si $(-N)^{\frac{c-1}{2}} - 1$ est divisible par $c$; dans le cas contraire, il ne pourra diviser $x^2 + N$, *ibid.*

Explication du caractère abrégé $\left(\frac{N}{c}\right)$, 186

§. II. *Recherche de la forme qui convient aux diviseurs de la formule* $t^2 + au^2$, 187

On prouve que tout diviseur de cette formule peut être représenté par une formule de même degré $py^2 + 2qyz + rz^2$, dans laquelle on a $pr - qq = a$, et $2q < p$ et $r$, 189

§. III. *Application de la théorie précédente à diverses formules* $t^2 + u^2$, $t^2 + 2u^2$, $t^2 - 2u^2$, &c. 190

On prouve que la somme de deux quarrés premiers entr'eux $t^2 + u^2$, ne peut avoir pour diviseur qu'une somme semblable $y^2 + z^2$, *ibid.*

Il en est de même des formules $t^2 + 2u^2$, $t^2 - 2u^2$, chacune n'admettant que des diviseurs semblables à elle-même, 191

Propriétés générales et caractéristiques des nombres premiers $8n+1$, $8n+3$, $8n+5$, $8n+7$, 196

Valeur du symbole $\left(\frac{2}{c}\right)$ selon l'espèce du nombre premier $c$, *ibid.*

§. IV. *Où l'on prouve que tout nombre entier est la somme de quatre ou d'un moindre nombre de quarrés,* 198

On démontre que $B$ et $C$ étant deux nombres donnés, il y a toujours des valeurs de $t$ et $u$ telles que $t^2-Bu^2-C$ est divisible par un nombre premier donné $A$, *ibid.*

Le produit de la formule $p^2+q^2+r^2+s^2$ par une formule semblable, donne un produit semblable, 200

Développement des différens cas du Théorême de Fermat sur les nombres polygones, 205

§. V. *De la forme linéaire qui convient aux diviseurs de la formule* $a^n \pm 1$, *a et n étant des nombres donnés,* 207

Tout nombre premier $p$ qui divise la formule $a^n+1$ sera de la forme $2nx+1$, ou au moins il devra diviser une formule plus simple $a^\omega+1$, dans laquelle $\omega$ est le quotient de $n$ divisé par un nombre impair, 208

Tout nombre premier $p$ qui divise la formule $a^n-1$ doit être compris dans la forme $nx+1$, ou au moins il sera diviseur de la formule $a^\omega-1$ dans laquelle $\omega$ est un sous-multiple de $n$, 211

Applications diverses où l'on détermine des nombres premiers très-grands, 213

§. VI. *Théorême contenant une loi de réciprocité qui existe entre deux nombres premiers quelconques,* 214

Si les deux nombres premiers $m$ et $n$ ne sont pas tous deux de la forme $4x-1$, on aura $\left(\frac{n}{m}\right)=\left(\frac{m}{n}\right)$; et s'ils sont tous deux de la forme $4x-1$, on aura $\left(\frac{n}{m}\right)=-\left(\frac{m}{n}\right)$, *ibid.*

Théorêmes divers dont plusieurs dépendent de la loi précédente, 221 — 224

On démontre par la même loi deux Conclusions générales auxquelles Euler est parvenu par voie d'induction dans ses *Opuscula analytica*, 225 — 226

§. VII. *Usage du Théorême précédent pour connoître si un nombre premier* c *divise la formule* $x^2+a$, 227

Algorithme très-simple pour cet objet, *ibid.*

Développement d'un grand nombre de cas où le nombre $x$ peut être déterminé *à priori*, 230

§. VIII. *De la manière de déterminer* x *pour que* $x^2+a$ *soit divisible par un nombre composé quelconque* N, 234

Nombre de solutions dont ce problême est susceptible, 237

§. IX. *Résolution des équations symboliques* $\left(\frac{x}{c}\right)=1$, $\left(\frac{x}{c}\right)=-1$, *c étant un nombre premier*, 239

§. X. *Recherche des formes linéaires qui conviennent aux diviseurs de la formule* $t^2+cu^2$, 243

Théorêmes par lesquels on détermine les formes linéaires des diviseurs de la formule $t^2+cu^2$, $c$ étant premier ou double d'un premier, 243–249

On détermine *a priori* les formes linéaires de ces mêmes diviseurs, lorsque $c$ est le produit de deux ou de plusieurs nombres premiers. — Conclusion générale qui prouve que les diviseurs linéaires de la formule $t^2+cu^2$ se partagent en différens groupes, chacun comprenant un même nombre de formes $2cx+a$ ou $4cx+a$, 253

Méthode abrégée pour trouver, par le moyen des diviseurs quadratiques, toutes les formes des diviseurs linéaires, 254

§. XI. *Explication des Tables III, IV, V, VI et VII*, 266

Ces Tables présentent pour chaque formule $t^2+cu^2$, comprise dans leurs limites, le système de ses diviseurs quadratiques et des diviseurs linéaires correspondans.

§. XII. *Suite de Théorêmes contenus dans les Tables précitées*, 278

On démontre en général, que si $4cx+a$ est l'une des formes linéaires qui répondent aux diviseurs de la formule $t^2+cu^2$, tout nombre premier compris dans la forme $4cx+a$ sera diviseur de la formule $t^2+cu^2$, et par conséquent sera de l'une des formes quadratiques qui répondent à ces formes linéaires, *ibid.*

On tire de-là autant de théorêmes particuliers qu'il y a de formes linéaires dans les Tables, 284

§. XIII. *Autres Théorêmes concernant les formes quadratiques des nombres*, 287

Tout nombre premier $A$ qui divise la formule $t^2 \pm au^2$ ne peut appartenir qu'à l'un des diviseurs quadratiques de cette formule, *ibid.*

Tout nombre premier $A$ qui est de la forme $y^2+az^2$ ne peut être qu'une fois de cette forme, 289

On détermine le nombre de manières dont un même nombre composé $A$ peut être de la forme $y^2+az^2$, d'où l'on déduit la solution d'un problême de Fermat, 293

Tout nombre $A$ premier, ou double d'un premier, compris dans la formule $py^2+2qyz+rz^2$, où $pr-q^2$ est un nombre positif, n'y peut être compris que d'une seule manière, sauf un ou deux cas prévus, 299

On détermine en combien de manières un nombre composé $P$, qui est diviseur de la formule $t^2+cu^2$, doit être compris dans les diviseurs quadratiques de cette formule, 301

§. XIV.

§. XIV. *Sur les moyens de trouver un nombre premier plus grand qu'un nombre donné,* 304

Tableau contenant diverses formules propres à exprimer des nombres premiers, si la condition correspondante est remplie, 307

Examen des formules les plus propres à offrir des nombres premiers. — Détermination de quelques-uns de ces nombres, 307—311

Explication de la propriété qu'ont certaines formules de contenir une suite assez étendue de nombres premiers, 311

§. XV. *Usage des Théorêmes précédens pour reconnoître si un nombre donné est premier, ou s'il ne l'est pas,* 313

On ajoute aux autres moyens connus le développement en fraction continue de la racine du nombre *A* ou d'un de ses multiples, 315

## TROISIÈME PARTIE.

### *Théorie des nombres considérés comme décomposables en trois quarrés.*

§. I. *Définition de la forme trinaire. Nombres et diviseurs quadratiques auxquels cette forme ne peut convenir,* 321

§. II. *Théorêmes relatifs aux diviseurs trinaires,* 325

Si un diviseur quadratique de la formule $t^2+cu^2$ est décomposable en trois quarrés, toute manière de faire cette décomposition, c'est-à-dire toute forme trinaire de ce diviseur, donnera une valeur correspondante de $c$, laquelle sera aussi de forme trinaire, 327

Réciproquement étant donnée une forme trinaire du nombre $c$, on pourra toujours trouver un diviseur quadratique de la formule $t^2+cu^2$, lequel aura une forme trinaire correspondante à la valeur donnée, 329

§. III. *Méthode directe pour trouver le diviseur trinaire de la formule* $t^2+cu^2$, *correspondant à une valeur trinaire donnée du nombre* $c$, 331

Etant donnée une valeur trinaire de $c$ dont les trois termes ne sont pas divisibles par un même nombre, on démontre 1°. qu'il ne peut y avoir qu'un seul diviseur quadratique qui réponde à cette valeur. 2°. Que ce diviseur ne pourra avoir qu'une forme trinaire correspondante à la valeur indiquée, sauf deux ou trois cas prévus où il peut avoir deux de ces formes, 331—340

§. IV. *Suite des Théorêmes relatifs aux diviseurs trinaires*, 344

Si le nombre $N$ est compris dans un diviseur trinaire de $t^2+cu^2$, réciproquement $c$ sera compris dans un diviseur trinaire de $t^2+Nu^2$. De plus, les valeurs trinaires de $N$ et $c$, déduites de chaque diviseur, seront identiques, 346

Si un même diviseur quadratique $py^2+2qyz+rz^2$ de la formule $t^2+cu^2$, se développe en plusieurs formes trinaires, tout nombre compris $N$ résultant des valeurs déterminées $y=\alpha$, $z=\zeta$, se développera en autant de formes trinaires, lesquelles seront différentes entr'elles, pourvu qu'on ait $N>\frac{1}{3}c$, 350

Autre Théorême sur la diversité des formes trinaires que prend un même nombre, en tant qu'il est compris dans un ou plusieurs diviseurs trinaires d'une même formule $t^2+cu^2$, 354

§. V. *Explication des Tables VIII, IX, X et XI*, 358

Ces Tables ont pour objet principal de développer les diverses formes trinaires dont chaque diviseur quadratique est susceptible, et de montrer leur correspondance avec les formes trinaires du nombre $c$.

Propriétés générales que présente l'inspection de ces Tables, 360, 362, 363, 364

§. VI. *Théorêmes comprenant la démonstration des propriétés observées dans les Tables*, 366

Théorêmes servant à établir la définition des diviseurs *réciproques* et des diviseurs *non réciproques*, 367

Si le nombre $c$ est premier, ou double d'un premier, tout diviseur quadratique de la formule $t^2+cu^2$ sera *réciproque*, 368

Si le nombre $c$ ou sa moitié, est un nombre composé, la formule $t^2+cu^2$ aura toujours au moins un diviseur quadratique *réciproque*, et au moins un *non réciproque*, 369

Tout diviseur de première espèce est un diviseur réciproque, 372

Tout diviseur réciproque de la formule $t^2+Nu^2$ est un diviseur de première espèce, et le nombre de ses formes trinaires sera $2^{i-1}$, $i$ étant le nombre de facteurs premiers impairs et inégaux qui divisent $N$, 374

On détermine d'une manière fort approchée combien il y a de nombres moindres que $N$, compris dans tout diviseur quadratique de la formule $t^2+Nu^2$, 385

Tout nombre impair, excepté les nombres $8n+7$, est la somme de trois quarrés, 398

Tout nombre entier est la somme de trois triangulaires, 399

Tout nombre double d'un impair est la somme de trois quarrés, *ibid.*

## QUATRIÈME PARTIE.

### MÉTHODES ET RECHERCHES DIVERSES.

§. I. *Théorèmes sur les puissances des nombres*, 401

L'aire d'un triangle rectangle en nombres entiers ne sauroit être égale à un quarré, *ibid.*
La somme de deux bi-quarrés ne peut être égale à un quarré, 404
La formule $x^4 + 2y^4$ ne peut être égale à un quarré, 405
Aucun nombre triangulaire, excepté 1, n'est égal à un bi-quarré, 406
La somme ou la différence de deux cubes, ne peut être égale à un cube, 407
Elle ne peut non plus être double d'un cube, 409
Aucun nombre triangulaire, excepté 1, n'est égal à un cube, *ibid.*

§. II. *Théorèmes concernant la résolution en nombres entiers de l'équation* $x^n - b = ay$, 411

Condition de possibilité, et réduction de l'équation, lorsque $a$ est un nombre premier, *ibid.*
Résolution de l'équation $x^n - 1 = ay$ lorsque $a$ est un nombre premier et $n$ un diviseur de $a - 1$, 413
Résolution de l'équation $x^{2n} + 1 = ay$ dans les mêmes cas, 415
Résolution de l'équation $x^n - b = ay$ dans les mêmes cas, 418
Résolution de la même équation en général, 420

§. III. *Méthode pour trouver le diviseur quadratique qui renferme le produit de plusieurs diviseurs quadratiques donnés*, 421

Formule pour avoir le produit de deux diviseurs quadratiques donnés, 422
Formule pour avoir le produit de deux diviseurs quadratiques semblables, 425
Diverses formes dont est susceptible le produit de plusieurs diviseurs quadratiques donnés, 427
Formule pour avoir la puissance $n$ d'un diviseur quadratique donné, 430

§. IV. *Résolution en nombres entiers de l'équation* $Ly^2 + Myz + Nz^2 = b\Pi$, $\Pi$ *étant le produit de plusieurs indéterminées ou de leurs puissances*, 435

Après avoir dégagé le second membre du facteur constant $b$, on fait voir comment la résolution de cette équation se déduit des développemens donnés dans le §. précédent, 436
Exemples divers, 436—440

§. V. *Démonstration d'une propriété relative aux diviseurs quadratiques de la formule* $t^2+au^2$, *a étant un nombre premier* $8n+1$, 441

On prouve d'abord, à la suite de plusieurs propositions subsidiaires, que l'équation $U^2=Py^2+2Qyz+Rz^2$, dans laquelle $PR-Q^2=a$, n'est susceptible que de deux solutions, lesquelles se réduisent à une seule, lorsque l'équation proposée est de la forme $U^2=2y^2+2yz+\frac{1}{2}(a+1)z^2$, 446

De-là on conclut que le nombre des diviseurs quadratiques $4n+1$ de la formule $t^2+au^2$ surpasse toujours d'une unité le nombre des diviseurs quadratiques $4n-1$ de la même formule, 449

§. VI. *Méthodes pour compléter la résolution en nombres entiers des équations indéterminées du second degré*, 451

Etant proposée l'équation $ay^2+byz+cz^2+dy+fz+g=0$, on fait disparoître les termes du premier degré, et on obtient la transformée $ay'^2+by'z'+cz'^2=H$. On donne ensuite une méthode générale et exempte de tâtonnement pour déduire des valeurs de $y'$ et $z'$ celles de $y$ et $z$ en nombres entiers, 453

Le succès de la méthode précédente étant fondé sur ce que les fractions à faire disparoître ont pour dénominateur $bb-4ac$, on se propose plus généralement de déterminer l'exposant $n$, tel qu'en faisant $(\varphi+\psi\sqrt{A})^n=F+G\sqrt{A}$, la quantité $\lambda F+\mu G+\nu$ soit divisible par un nombre premier quelconque $\omega$, 454

On détermine ensuite directement la valeur du même exposant, telle que $\lambda F+\mu G+\nu$ soit divisible par une puissance donnée du nombre premier $\omega$, 455

§. VII. *Méthode de Fermat pour la résolution de l'équation* $y^2=a+bx+cx^2+dx^3+ex^4$ *en nombres rationnels*, 458

Si l'équation proposée est telle que $a$ ou $e$ soit un quarré, on donne le moyen d'en trouver successivement tant de solutions qu'on voudra, *ibid.*

On applique cette méthode à deux problèmes particuliers, 460—461

## ADDITIONS.

*Introduction*, *Art.* X, 463

———— *Art.* XXVI *et* XXVIII, 464

*Première Partie*, §. XII, ibid.

*Seconde Partie*, n°. 230, ibid.

*Troisième Partie*, n°. 273, 465

———— *Théor.* X, ibid.

———— *Théor.* XVI, 466

## TABLES.

*Table I.* Expressions les plus simples des formules $Ly^2 + 2Myz + Nz^2$, pour toutes les valeurs du nombre non-quarré $A = M^2 - LN$, depuis $A = 2$ jusqu'à $A = 136$.

*Table II.* Expressions les plus simples des formules $Ly^2 + Myz + Nz^2$, où $M$ est impair, pour toutes les valeurs du nombre non-quarré $B = M^2 - 4LN$, depuis $B = 5$ jusqu'à $B = 305$.

*Table III.* Diviseurs quadratiques et linéaires de la formule $t^2 - au^2$, pour tout nombre $a$ non-quarré ni divisible par un quarré, depuis $a = 2$ jusqu'à $a = 79$.

*Table IV.* Diviseurs quadratiques et linéaires de la formule $t^2 + au^2$, pour tout nombre $a$ de forme $4n + 1$, non-quarré ni divisible par un quarré, depuis $a = 1$ jusqu'à $a = 105$.

*Table V.* Diviseurs quadratiques et linéaires de la formule $t^2 + au^2$, pour tout nombre $a$ de forme $4n - 1$, non divisible par un quarré, depuis $a = 3$ jusqu'à $a = 103$.

*Table VI.* Diviseurs quadratiques et linéaires de la formule $t^2 + 2au^2$, pour tout nombre $a$ de forme $4n + 1$, non-quarré ni divisible par un quarré depuis $a = 1$ jusqu'à $a = 53$.

*Table VII.* Diviseurs quadratiques et linéaires de la formule $t^2 + 2au^2$, pour tout nombre $a$ de forme $4n - 1$, non divisible par un quarré, depuis $a = 3$ jusqu'à $a = 51$.

*Table VIII.* Diviseurs quadratiques $4n + 1$ de la formule $t^2 + cu^2$, pour tout nombre $c$ de forme $4n + 1$, depuis $c = 1$ jusqu'à $c = 213$, avec les formes trinaires dont ils sont susceptibles, et les valeurs trinaires correspondantes du nombre $c$.

*Table IX.* Diviseurs quadratiques $4n + 2$ de la formule $t^2 + cu^2$, pour tout nombre $c$ de forme $8n + 3$, depuis $c = 3$ jusqu'à $c = 219$, avec les formes trinaires dont ils sont susceptibles, et les valeurs trinaires correspondantes du nombre $c$.

*Table X.* Diviseurs quadratiques $8n + 1$ et $8n + 3$ de la formule $t^2 + 2au^2$, pour tout nombre $a$ de forme $4n + 1$, depuis $a = 1$ jusqu'à $a = 117$, avec les formes trinaires de ces diviseurs, et les valeurs correspondantes du nombre $2a$.

*Table XI.* Diviseurs quadratiques $8n + 3$ et $8n + 5$ de la formule $t^2 + 2au^2$, pour tout nombre $a$ de forme $4n - 1$, depuis $a = 3$ jusqu'à $a = 123$, avec

# ERRATA.

PAGE 8, ligne 3, $\alpha^{m-1}\ldots\zeta^{n-1}\ldots\gamma^{p-1}$; lisez $\alpha^{m}\ldots\zeta^{n}\ldots\gamma^{p}$,

Page 15, lig. 11, $n\cdot\frac{1}{3}\cdot\frac{4}{5}\cdot\frac{5}{7}\ldots\frac{\omega-1}{\omega}$; lis. $n\cdot\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{6}{7}\ldots\frac{\omega-1}{\omega}$,

Page 18, lig. 22, 170; *lis.* 169.

Page 20, *effacez* 527, qui n'est pas un nombre premier, et dans la colonne verticale, au lieu de 111, 127, 141, 156, 170; *lis.* 110, 126, 140, 155, 169.

Page 30, avant-dernière ligne, $\frac{p^{000}}{000}$; lis. $\frac{p^{000}}{q^{000}}$.

Page 34, dans les dernières lignes, *changez* les $y$ en $u$.

Page 64, lig. 3, $\frac{455}{38}$; *lis.* $\frac{455}{33}$.

Page 65, au titre, $Ay^2$; lis. $ay^2$.

Page 92, lig. 6, $\frac{p_n}{n}$; lis. $\frac{p_n}{q_n}$.

Page 97, lig. 10, $fx^2+gz+h$; lis. $fx^2+gx+h$.

Page 117, lig. 1, *mettez* une virgule à la place du point qui précède *Il est clair.*

Page 150, dernière ligne, $=0$; *lis.* $Z=0$.

Page 157, lig. dernière, $\frac{F'\left(\frac{p}{q}\right)}{qF\left(\frac{p}{q}\right)}$; lis. $\frac{F'\left(\frac{p}{q}\right)}{q^2F\left(\frac{p}{q}\right)}$.

Page 161, lig. 21, et que la fraction; *lis.* et qu'ainsi la fraction.

Page 199, lig. 15, $C_a$; lis. $C^a$.

Page 207, au titre $a\pm1$; *lis.* $a^n\pm1$.

*Ibid.* lig. 23, $a'=1$; lis. $a^{\pi,n}=1$.

Page 251, lig. 5, la première; *lis.* la seconde.

*Ibid.* lig. 12, la seconde; *lis.* la première.

Page 283, lig. 8, $\left(\frac{P}{\ }\right)$; lis. $\left(\frac{P}{\zeta}\right)$.

Page 288, lig 25, $\theta$ étant un diviseur de $c$; *ajoutez* non divisible par $\alpha$.

Page 301, lig. 12, *impairs, i;* lis. *impair, si.*

*Ibid.* A l'arrivée du Théorême n°. 243, *ajoutez* : on suppose que $P$ et $c$ n'ont aucun facteur quarré commun.

Page 388, lig. 5, $\frac{\zeta^2}{\ }$; lis. $\frac{\zeta^2}{c}$.

Page 353, lig 15, $-\frac{q}{3p}$; lis. $-\frac{q}{3\sqrt{p}}$.

Page 354, Théorême X, *ajoutez* à l'énoncé, *sans supposer* $z=0$.

Page 355, lig. 5, $c'$; lis. $c$.

Page 372, lig. 22, $f^2\mu^2+g^n\lambda^2$; lis. $f^2\mu^2+g^2\lambda^2$,

Page 373, lig. 16, de forme trinaire; *lis.* des formes trinaires.

Page 383, dans la note, ce V$^{e}$ Cas; *lis.* ce VI$^{e}$ Cas.

Page 387, lig 28, si on appelle $\zeta$; *lis.* si on appelle $Z$.

Page 391, lig. antepénultième, sont nécessairement différens entr'eux; *ajoutez* sauf le cas où l'on auroit $c^2=\varphi^2+N\psi^2$.

Page 408, lig 14 et 16, $\sqrt[3]{\ }$; *lis.* $\sqrt[5]{\ }$.

Page 446, lig. 6, $v^2$; lis. $U^2$.

Page 448, lig. 9, $y + 2yz$; lis. $y^2 + 2yz$.

*Ibid.* lig 26, $2y^2 + 2yz + (a+1)z^2$; lis $2y^2 + 2yz + \frac{1}{2}(a+1)z^2$.

Table IV, dans la note, les diviseurs quadratiques; *ajoutez* $4n+1$; voyez d'ailleurs le n° 305.

Table VI, $296x+1$, 9, 11.... 289; 299; *lis.* $296x+1$, 3, 9, 11.... 289.

Table VIII, formule $t^2 + 161u^2$; *ajoutez* aux diviseurs non-décomposables la formule $9y^2 + 2yz + 18z^2$.

Table X, à l'article de la formule $t^2 + 50u^2$, ajoutez ce qui suit :

$$\left.\begin{matrix} 25+16+9 \\ 25+25 \end{matrix}\right\} 9y^2+4yz+6z^2 = \left\{\begin{matrix} (2y+z)^2+(2y-z)^2+(y+2z)^2 \\ (2y+z)^2+(2y+z)^2+(y-2z)^2 \end{matrix}\right.$$

$$25+25 \mid 3y^2+4yz+18z^2 = (y+4z)^2+(y-z)^2+(y-z)^2.$$

---

ESSAI

# ESSAI

SUR

# LA THÉORIE DES NOMBRES.



## INTRODUCTION,

*Contenant des notions générales sur les Nombres.*

NOTRE objet, dans cette introduction, est de présenter quelques considérations générales sur la nature des nombres, et particulièrement sur celle des nombres premiers. Mais avant tout, nous croyons devoir nous occuper de quelques propositions fondamentales, dont la démonstration ne se trouve pas dans les traités ordinaires d'Arithmétique, ou du moins n'y est présentée que d'une manière peu rigoureuse.

I. Nous examinerons d'abord pourquoi le produit de deux nombres demeure le même, en changeant l'ordre des facteurs, c'est-à-dire pourquoi l'on a $A \times B = B \times A$.

Un moyen très-simple de se convaincre de la vérité de cette proposition, consiste à faire ou imaginer une figure rectangulaire, qui contienne plusieurs rangées égales de quarrés égaux ou de cercles égaux. Si vous faites $A$ rangées chacune de $B$ quarrés, la même figure vous offrira $B$ rangées chacune de $A$ quarrés. Le nombre total des quarrés sera donc également représenté par $B \times A$ et par $A \times B$; de sorte que ces produits sont nécessairement égaux.

Cette démonstration nous paroît à-la-fois claire, générale et exacte; cependant si on lui reproche d'être fondée sur des notions

d'étendue étrangères à la science des nombres, voici comment on pourra y suppléer.

Soit $A$ le plus grand des nombres $A$ et $B$, soit $C$ lenr différence, et en conséquence $A = B + C$. On accordera aisément que le produit de $A$ par $B$ est composé du produit de $B$ par $B$, et du produit de $C$ par $B$ ; de sorte qu'en écrivant le multiplicateur le dernier, on a $A \times B = B \times B + C \times B$. Mais le produit de $B$ par $A$ ou par $B + C$ est composé aussi de $B$ pris $B$ fois et de $B$ pris $C$ fois, de sorte qu'on a $B \times A = B \times B + B \times C$. De-là on voit que le produit $A \times B$ sera le même que le produit $B \times A$, si le produit partiel $C \times B$ est égal à $B \times C$. Mais par la même raison, l'égalité entre $CB$ et $BC$ se prouvera par l'égalité entre denx produits plus petits $CD$ et $DC$, et en continnant ainsi, on parviendra nécessairement soit au cas où les deux facteurs sont éganx, soit au cas où l'un d'eux est égal à l'unité. Dans le premier cas, l'égalité est manifeste ; dans le second, elle se conclut de ce que $H \times 1$ est la même chose que $1 \times H$, l'un et l'antre étant égal à $H$. Donc le produit $A \times B$ est toujours égal au produit $B \times A$.

II. On suppose ordinairement, qu'en multipliant un nombre donné $M$ par un autre nombre $N$ qui est lui-même le produit des deux facteurs $A$ et $B$, il revient au même de multiplier $M$ par $N$ tout d'un coup, ou bien de multiplier d'abord $M$ par $A$, ensuite le produit par $B$. Cette conclusion, considérée en général, peut cependant ne paroître ni absolument évidente, ni une suite de la proposition précédente.

Pour la démontrer, imaginons un assemblage de sphères égales, ou de cubes égaux rangés en forme parallélipipède, de manière qu'on en compte un nombre $M$ dans le sens de la longueur, un nombre $A$ dans le sens de la largeur, et un nombre $B$ dans le sens de la hauteur ; il y anra, cela posé, différentes manières de tronver le nombre total des sphères, et ces différentes manières donneront certainement le même résultat.

Si on ne considère d'abord qu'une sphère dans la hauteur, le nombre des sphères résultera du produit des autres dimensions $A$ et $B$, et sera $A \times B$. Il faudra ensuite multiplier ce produit

par le nombre de sphères comprises dans la hauteur, c'est-à-dire par $M$, et le nombre total des sphères conclu de ces deux opérations, sera $A \times B \times M$.

Mais dans la forme que nous supposons, on peut prendre également $B$ pour la hauteur, $M$ et $A$ pour les autres dimensions. Raisonnant donc sur ces nombres comme sur les précédens, on auroit pour le nombre total des sphères $M \times A \times B$.

On doit donc avoir $A \times B \times M = M \times A \times B$. Mais $A \times B = N$ et $N \times M = M \times N$, donc $M \times N$ ou $M \times AB = M \times A \times B$. C'est la proposition que nous voulions démontrer.

On pourroit démontrer la même chose, mais d'une manière peut-être moins claire, par une simple figure rectangulaire. Imaginons $M$ quarrés égaux dans la largeur et $N$ dans la longueur. Le nombre total des quarrés sera $M \times N$. Supposons ensuite que $N$ est le produit des deux nombres $A$ et $B$, nous pourrons concevoir dans la longueur totale $N$ autant de fois la longueur partielle $A$ que le nombre $B$ contient d'unités. Mais le nombre de quarrés qui, dans la figure rectangulaire, répond à chaque longueur partielle $A$, est $M \times A$ : donc puisque la longueur partielle $A$ est contenue $B$ fois dans la longueur totale $N$, il faut multiplier le nombre $M \times A$ par $B$, et on aura $M \times A \times B$ pour le nombre de quarrés contenus dans la figure totale. Donc le nombre $M \times N$ déduit d'une seule multiplication, est égal au nombre $M \times A \times B$ qui résulte de deux multiplications.

III. D'après ces deux propositions, on démontrera facilement que *le produit de tant de facteurs que l'on voudra, demeure toujours le même, en quelqu'ordre que les facteurs soient multipliés.*

Pour prouver, par exemple, que le produit $A \times B \times C \times D$ est égal au produit $CADB$, je commence par faire en sorte que la même lettre occupe la dernière place dans les deux. Or on a, en vertu des propositions précédentes, $A \times B \times C = A \times C \times B$; donc $ABCD = ACBD$; considérant ensuite $AC$ comme un seul nombre, on aura $AC \times B \times D = AC \times D \times B$. Ainsi la lettre $B$ est à la dernière place dans ce produit, comme elle l'est dans l'autre produit donné $CADB$; ôtant cette dernière lettre, il ne

reste plus à prouver que l'égalité $ACD = CAD$, or elle suit de ce que $AC = CA$.

IV. *Le produit de deux nombres* A *et* B *est divisible par tout nombre premier qui divise exactement l'un ou l'autre des facteurs* A *et* B.

Car soit $\theta$ un nombre premier qui divise $B$, et soit en conséquence $B = C \times \theta$, on aura $AB = AC \times \theta$; donc $AB$ divisé par $\theta$ donne le quotient exact $AC$.

V. *Si le nombre $\theta$ divise à la fois les deux nombres* A *et* B, *il divisera la somme et la différence de deux multiples quelconques de ces nombres.*

Car si l'on a $A = A'\theta$, $B = B'\theta$, partant $mA \pm nB = mA'\theta \pm nB'\theta$, cette quantité divisée par $\theta$ donnera le quotient exact $mA' \pm nB'$.

VI. *Tout nombre premier qui ne divise ni l'un ni l'autre des facteurs* A *et* B, *ne peut diviser leur produit* AB.

Cette proposition étant l'une des plus importantes de la théorie des nombres, nous donnerons à sa démonstration tout le développement *nécessaire*.

Soit, s'il est possible, $\theta$ un nombre premier qui ne divise ni $A$ ni $B$, mais qui divise le produit $AB$; soit que $A$ soit plus grand ou plus petit que $\theta$, on pourra supposer qu'en divisant $A$ par $\theta$, on a le quotient $m$ (qui peut être zéro) et le reste $A'$; on aura donc $A = m\theta + A'$; on aura semblablement $B = n\theta + B'$. Donc $AB = mn\theta\theta + nA'\theta + mB'\theta + A'B'$. Cette quantité, d'après l'hypothèse, doit être divisible par $\theta$, et comme la partie $mn\theta\theta + nA'\theta + mB'\theta$ se divise d'elle-même par $\theta$, il faudra donc que l'autre partie $A'B'$ soit également divisible par $\theta$; ainsi nous pourrons faire $A'B' = \theta C'$.

Dans ce premier résultat, nous remarquerons, 1°. que $A'$ et $B'$ ne sont zéro, ni l'un ni l'autre, parce que $A$ et $B$ sont supposés non-divisibles par $\theta$; 2°. que $A'$ et $B'$ étant des restes de division sont moindres que le diviseur $\theta$; 3°. qu'aucun des nombres $A'$, $B'$ ne peut être égal à l'unité; car si on avoit $A' = 1$, le produit $A'B'$

deviendroit $B'$; or $B'$ étaut $< \theta$, il est impossible que $B'$ soit divisible par $\theta$.

Nous avons donc deux nombres entiers $A'$, $B'$, tous deux plus grands que l'unité, et tous deux moindres que $\theta$, dont le produit est divisible par $\theta$, de sorte qu'on a $A' B' = \theta C'$. Voyons les conséquences qui en résultent.

Puisque $A'$ est moindre que $\theta$, on peut diviser $\theta$ par $A'$; soit $m$ le quotient et $A''$ le reste, on aura $\theta = m A' + A''$. Donc $\theta \times B' = m \times A' \times B' + A'' \times B'$. Le premier membre est divisible par $\theta$, il faut donc que le second le soit aussi : mais la partie $m \times A' \times B'$ est divisible d'elle-même par $\theta$, puisque $A' B' = C \theta$; donc l'autre partie $A'' B'$ doit être encore divisible par $\theta$.

Le nombre $A''$, qui est un reste de division, est moindre que le diviseur $A'$; il ne peut d'ailleurs être zéro, car si cela étoit, $\theta$ seroit divisible par $A'$, et ne seroit plus un nombre premier. Donc du produit $A' B'$, supposé divisible par $\theta$, on tire un autre produit $A'' B'$ divisible encore par $\theta$, lequel est plus petit que $A' B'$ et cependant n'est pas zéro.

En suivant le même raisonnement, on déduira du produit $A'' B'$ un autre produit $A''' B'$ ou $A'' B''$, encore plus petit, et qui sera toujours divisible par $\theta$ sans être zéro.

Et en continuant la suite de ces produits décroissans, on parviendra nécessairement à un nombre moindre que $\theta$. Or il est impossible qu'un nombre moindre que $\theta$ et qui n'est pas zéro, soit divisible par $\theta$; donc l'hypothèse d'où l'on est parti est impossible.

Donc si les nombres $A$ et $B$ ne sont divisibles, ni l'un ni l'autre, par le nombre premier $\theta$, leur produit $AB$ ne pourra non plus être divisible par $\theta$.

VII. La doctrine des incommensurables repose entièrement sur le principe qu'on vient de démontrer. En effet, s'il existoit, par exemple, une fraction rationnelle $\frac{m}{n}$ égale à $\sqrt{2}$, il faudroit que $\frac{m^2}{n^2}$ fût égale à 2; donc $m^2$ devroit être divisible par chacun des

nombres premiers qui divisent $n$. Mais la fraction $\frac{m}{n}$ étant censée irréductible, $m$ n'a aucun diviseur commun avec $n$; donc en vertu du théorême précédent $m^2$ ne peut avoir non plus aucun diviseur commun avec $n$; donc il est impossible qu'on ait $\frac{m^2}{n^2}=2$.

En général, une puissance quelconque du nombre $a$ ne peut avoir pour diviseurs d'autres nombres premiers que ceux qui divisent $a$; et ainsi, si on ne peut trouver l'entier $x$ tel que $x^n=b$, $b$ étant un nombre entier donné, on ne pourra non plus satisfaire à l'équation $\frac{x^n}{y^n}=b$.

VIII. *Un nombre quelconque* N, *s'il n'est pas premier, peut être représenté par le produit de plusieurs nombres premiers* $\alpha, \beta, \gamma$, &c. *élevés chacun à une puissance quelconque, de sorte qu'on peut toujours supposer* $N=\alpha^m \beta^n \gamma^p$, &c.

En effet, la méthode à suivre pour opérer cette décomposition, consiste à essayer la division du nombre $N$ successivement par chacun des nombres premiers 2, 3, 5, 7, &c. (1). Lorsque la division réussit par le nombre premier $\alpha$, on la répète autant de fois qu'il est possible, $m$ fois en général; et en appelant le dernier quo-

(1) On reconnoît à la seule inspection, si un nombre donné est divisible par 2, 3, ou 5 : à l'égard des autres nombres premiers, il n'y a guère de règle plus simple que la division effective. Cependant comme le produit des trois nombres 7, 11, 13 est 1001, il s'ensuit que 1000 divisé par l'un de ces nombres, laisse le reste $-1$, que $(1000)^2$ laisse le reste $+1$, $(1000)^3$ le reste $-1$, et ainsi alternativement. De-là on déduit un procédé fort simple, pour savoir si un nombre donné est divisible par l'un des nombres premiers 7, 11, 13, ou par le produit de deux d'entr'eux; soit, par exemple, le nombre 22473809514, après l'avoir partagé en tranches de trois chiffres, de gauche à droite, je fais une somme des tranches 1ère, 3e, 5e, &c., et une des autres tranches. Je soustrais la seconde somme 831 de la première 987, et j'ai la différence $+156$. Cette différence n'est divisible ni par 7 ni par 11, mais elle est divisible par 13; donc le nombre proposé n'est divisible ni par 7 ni par 11, mais il est divisible par 13. En général, la différence ainsi trouvée, prise pour dividende, donnera le même reste que le nombre proposé.

tient $P$, on aura $N = \alpha^m P$. Le nombre $P$ ne pouvant plus être divisé par $\alpha$, il est inutile d'essayer la division de $P$ par un nombre premier moindre que $\alpha$; car si $P$ étoit divisible par $\theta$ moindre que $\alpha$, il est clair que $N$ seroit aussi divisible par $\theta$, ce qui est contraire à la supposition. On ne doit donc essayer de diviser $P$ que par les nombres premiers plus grands que $\alpha$; on trouvera ainsi successivement $P = 6^n Q$, $Q = \gamma^p R$, &c. ce qui donnera $N = \alpha^m 6^n \gamma^p$, &c.

IX. *Si après avoir essayé la division d'un nombre donné* N *par les nombres premiers successifs* 2, 3, 5, 7... *jusqu'à* $\sqrt{N}$, *on n'en trouve aucun qui divise* N, *on en conclura avec certitude que* N *est un nombre premier.*

Car supposons que $N$ soit divisible par un nombre premier $\theta > \sqrt{N}$, on auroit donc, en appelant $P$ le quotient, $N = \theta P$. Mais puisque $\theta$ est $> \sqrt{N}$, on aura $P = \frac{N}{\theta} < \frac{N}{\sqrt{N}} < \sqrt{N}$; donc $N$ seroit divisible par un nombre $P$ moindre que $\sqrt{N}$, donc à plus forte raison il seroit divisible par un nombre premier $< \sqrt{N}$, ce qui est contre la supposition.

On peut donc trouver de cette manière si un nombre donné $N$ est premier ou s'il ne l'est pas. Mais quoique cette méthode soit susceptible de quelques abrégés dont nous ferons mention ci-après, elle est en général longue et fastidieuse. Aussi plusieurs Mathématiciens ont-ils jugé convenable de construire des tables de nombres premiers plus ou moins étendues. La manière la plus simple de construire ces tables, est de commencer par écrire de suite tous les nombres impairs 1, 3, 5, 7, 9, 11, &c. jusqu'à 100000, ou telle autre limite qu'on peut se proposer. Cette suite étant formée, on en efface successivement tous les multiples de 3, tous ceux de 5, tous ceux de 7, &c. en conservant seulement les premiers termes 3, 5, 7, &c. non effacés par les opérations antérieures. De cette manière, il est visible que tous les nombres restans n'ont d'autres diviseurs qu'eux-mêmes, et qu'ainsi ils sont des nombres premiers (1).

(1) On trouvera à la fin de cette introduction, une petite table de tous les nombres premiers au-dessous de 1000.

X. Un nombre donné $N$ étant réduit à la forme $\alpha^m \beta^n \gamma^p \ldots$ il est clair qu'il aura pour diviseurs tous les termes du produit développé $(1+\alpha+\alpha^2\ldots+\alpha^{m-1})(1+\beta+\beta^2\ldots+\beta^{n-1})(1+\gamma+\gamma^2\ldots+\gamma^{p-1})$ &c. Donc le nombre de tous ses diviseurs sera $(m+1)(n+1)(p+1)$ &c.

Par exemple, puisqu'on a $360=2^3.3^2.5^1$, les diviseurs de 360 sont au nombre de 4.3.2 ou de 24.

XI. Réciproquement il est facile de trouver un nombre qui ait autant de diviseurs qu'on voudra. Cherchons, par exemple, un nombre qui ait 36 diviseurs ; on décomposera 36 en facteurs (premiers ou non), tels que 4, 3, 3; on diminuera chaque facteur d'une unité, ce qui donnera 3, 2, 2; d'où l'on conclura que $\alpha^3 \beta^2 \gamma^2$ est la forme d'nn nombre qui a 36 divisenrs, $\alpha$, $\beta$, $\gamma$ étant des nombres premiers. Le plus simple de ces nombres est $2^3.3^2.5^2=1800$.

XII. Si on cherche en combien de manières le nombre $N=\alpha^m \beta^n \gamma^p$, &c. peut être le produit de deux facteurs $A$ et $B$; on trouvera que ce nombre est $\frac{1}{2}(m+1)(n+1)(p+1)$, &c. Car chaque diviseur $A$ est censé accompagné de son inverse $\frac{N}{A}$ ou $B$, et ainsi le nombre des quantités $AB$ ou $BA$ est la moitié de celui des diviseurs de $N$.

Si le nombre $N$ étoit un quarré, tous les exposans $m, n, p$, &c. seroient pairs, et alors la moitié du produit $(m+1)(n+1)(p+1)$, &c. contiendroit la fraction $\frac{1}{2}$ pour laquelle il faudroit prendre l'unité.

XIII. Si on veut que les deux facteurs dans lesquels on décompose le nombre $N$ soient premiers entr'eux, alors le nombre des combinaisons ne dépend plus des exposans $m, n, p$, &c., et il est le même que si le nombre $N$ étoit $\alpha\beta\gamma\delta$ &c.; de sorte qu'en appelant $k$ le nombre des facteurs $\alpha$, $\beta$, $\gamma$, &c., on aura $2^{k-1}$ pour le nombre de manières de partager $N$ en deux facteurs premiers entr'eux.

Par exemple, le nombre 1800 peut se partager de 18 manières en deux facteurs, mais il ne se peut partager que de quatre

quatre manières en deux facteurs premiers entr'eux ; car on a $1800 = 2^3 . 3^2 . 5^2$, et $2^{3-1} = 4$.

XIV. Si l'on prend la suite des nombres naturels 1,2,3,4,5,6,&c. et qu'on désigne par $\int n$ la somme des diviseurs du nombre $n$, on aura successivement :

$$\int 1 = 1$$
$$\int 2 = 1 + 2$$
$$\int 3 = 1 + 3$$
$$\int 4 = 1 + 2 + 4$$
$$\int 5 = 1 + 5$$
$$\int 6 = 1 + 2 + 3 + 6$$
$$\int 7 = 1 + 7$$
$$\int 8 = 1 + 2 + 4 + 8$$
$$\int 9 = 1 + 3 + 9$$
$$\int 10 = 1 + 2 + 5 + 10$$
&c.

Ces sommes paroissent suivre une loi très-irrégulière, puisqu'à côté d'un nombre premier, qui n'a que deux diviseurs, on rencontre souvent un nombre composé qui en a un très-grand nombre ; cependant Euler a fait voir que cette loi peut être assignée d'une manière assez simple et analogue à la loi des suites récurrentes. Voyez le tome V des nouveaux Commentaires de Pétersbourg. Voyez aussi l'Introduction à l'Analyse des Infinis, traduite par J. B. Labey, tom. 1, pag. 355.

XV. Tout nombre premier, excepté 2 et 3, est compris dans la formule $6x \pm 1$. En effet, si l'on divise un nombre impair par 6, le reste ne peut être que l'un des nombres 1, 3, 5, ou (parce que le reste 5 est censé le même que le reste $-1$), 1, 3, $-1$. Donc tout nombre impair peut être représenté par l'une des formules $6x+1$, $6x+3$, $6x-1$. La seconde ne peut convenir aux nombres premiers, puisqu'elle est divisible par 3, et que 3 est excepté ; donc tout nombre premier, hors 2 et 3, est compris dans la formule $6x \pm 1$.

Il ne s'ensuit pas réciproquement, que tout nombre compris dans la formule $6x \pm 1$ soit un nombre premier; on trouveroit que cela n'a pas lieu lorsque $x = 4, 6$, &c.

XVI. En général, il n'existe aucune formule algébrique qui ne représente que des nombres premiers. Car soit, par exemple, la formule $P = ax^3 + bx^2 + cx + d$, et supposons qu'en faisant $x = k$, la valeur de $P$ soit égale au nombre premier $p$; si on fait $x = k + py$, $y$ étant un entier quelconque, on aura

$$P = p + (3ak^2 + 2bk + c)\,py + (3ak + b)\,p^2y^2 + ap^3y^3.$$

D'où l'on voit que $P$ n'est pas un nombre premier, puisqu'il est divisible par $p$, et différent de $p$.

Il est néanmoins quelques formules remarquables par la multitude de nombres premiers qui y sont contenus: telle est la formule $x^2 + x + 41$ dont Euler fait mention dans les Mémoires de Berlin (an. 1772, pag. 36), et dans laquelle, si l'on fait successivement $x = 0, 1, 2, 3$, &c. on a la suite 41, 43, 47, 53, 61, 71, &c. dont les quarante premiers termes sont des nombres premiers.

On peut citer dans ce même genre la formule $x^2 + x + 17$, dont les dix-sept *premiers* termes sont des nombres premiers; la formule $2x^2 + 29$, dont les 29 premiers le sont, et une foule d'autres.

XVII. Si on ne peut pas trouver de formule algébrique qui renferme uniquement des nombres premiers, à plus forte raison n'en peut-on pas trouver une qui renferme absolument tous ces nombres, et qui soit l'expression de leur loi générale. Cette loi paroît très-difficile à trouver d'une manière quelconque, et il n'y a guère d'espérance qu'on y parvienne jamais. Cela n'empêche pas qu'on ne puisse découvrir et démontrer un grand nombre de propriétés générales des nombres premiers, lesquelles répandent un grand jour sur leur nature.

Et d'abord nous pouvons démontrer rigoureusement que la multitude des nombres premiers est infinie.

Car si la suite des nombres premiers 1, 2, 3, 5, 7, 11, &c. étoit

finie, et que $p$ fût le dernier ou le plus grand de tous, il faudroit qu'un nombre quelconque $N$ fût toujours divisible par quelqu'un des nombres premiers $2.3.5.7....p$. Mais si on représente par $P$ le produit de tous ces nombres (1), il est clair qu'en divisant $P+1$ par l'un quelconque des nombres premiers jusqu'à $p$, le reste sera $+1$; donc l'hypothèse que $p$ est le plus grand des nombres premiers ne sauroit avoir lieu; donc la multitude des nombres premiers est infinie.

Cette proposition se prouve encore d'une manière directe et fort élégante, en faisant voir que la somme de la suite $\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+$ &c. est infinie. Voyez l'*Introd. in Anal. infin.* pag. 235.

XVIII. Tous les nombres impairs s'expriment par la formule $2x+1$, laquelle selon que $x$ est pair ou impair contient les deux formes $4x+1$ et $4x-1$. De-là deux grandes divisions des nombres premiers, l'une comprenant les nombres premiers $4x+1$, savoir 1, 5, 13, 17, 29, 37, 41, 53, 61, 73, &c., l'autre comprenant les nombres premiers $4x-1$, savoir 3, 7, 11, 19, 23, 31, 43, 47, 59, &c.

La forme générale $4x+1$ se subdivise en deux autres formes $8x+1$ et $8x+5$ ou $8x-3$. De même la forme $4x-1$ se subdivise en deux autres $8x+3$ et $8x+7$ ou $8x-1$; de sorte

(1) Si l'on admet successivement 1, 2, 3, &c., facteurs dans le produit $P$, on trouvera que le nombre $P+1$ prend les valeurs 3, 7, 31, 211, 2311, 30031, &c. Les cinq premiers termes sont des nombres premiers, ce qui pourroit faire présumer que les suivans le sont; mais cette conjecture est bientôt anéantie, en examinant le sixième terme 30031 qu'on trouve être le produit de 59 par 509. En général, c'est un problême difficile, et non encore résolu, de trouver un nombre premier plus grand qu'un nombre donné. Fermat avoit annoncé (mais sans dire qu'il en eût la démonstration) que la formule $2^x+1$ donnoit toujours des nombres premiers, pourvû qu'on prît pour $x$ un terme de la progression double 1, 2, 4, 8, 16, &c. Cette formule, qui auroit fourni une solution très-simple du problême mentionné, s'est trouvée en défaut; car suivant la remarque d'Euler, si l'on fait $x=32$, on a $2^x+1=641.6700417$.

B 2

qu'on peut réduire tous les nombres premiers à ces quatre formes principales,

$8x+1$.... 1, 17, 41, 73, 89, 97, 113, 137, &c.
$8x+3$.... 3, 11, 19, 43, 59, 67, 83, 107, &c.
$8x-3$ ou $8x+5$.... 5, 13, 29, 37, 53, 61, 101, 109, &c.
$8x-1$ ou $8x+7$.... 7, 23, 31, 47, 71, 79, 103, 127, &c.

XIX. Nous avons déjà vu que les nombres premiers considérés par rapport aux multiples de 6, sont de l'une des deux formes $6x+1$, $6x-1$; dans celles-ci $x$ peut être pair ou impair, et de-là résultent, par rapport aux multiples de 12, les quatre formes $12x+1$, $12x+5$, $12x-5$, $12x-1$, chacune renfermant une infinité de nombres premiers.

En général, $a$ étant un nombre donné quelconque, tout nombre impair peut être représenté par la formule $4ax \pm b$, dans laquelle $b$ est impair et moindre que $2a$. Si parmi toutes les valeurs possibles de $b$ on retranche celles qui ont un commun diviseur avec $a$, les formes restantes $4ax \pm b$ comprendront tous les nombres premiers partagés, à l'égard des multiples de $4a$, en autant d'espèces ou formes que $\pm b$ aura de valeurs différentes. Ainsi en faisant $a=15$, on aura les seize formes différentes

$60x+1$, $60x+7$, $60x+11$, $60x+13$
$60x-1$, $60x-7$, $60x-11$, $60x-13$
$60x+17$, $60x+19$, $60x+23$, $60x+29$
$60x-17$, $60x-19$, $60x-23$, $60x-29$

dont chacune comprend une infinité de nombres premiers, et qui par leur réunion renferment la totalité de ces nombres (2, 3 et 5 exceptés).

XX. Ces divisions générales nous portent à considérer une progression arithmétique quelconque

..... $-2A+B$, $-A+B$, $B$, $A+B$, $2A+B$, &c.

dont le terme général est $Ax+B$. Soit $\theta$ un nombre premier non-diviseur de $A$, on pourra toujours trouver une infinité de valeurs de $x$ telles que $\frac{Ax+B}{\theta}$ soit un entier; car si on appelle $\alpha$ la plus

petite de ces valeurs (1), et qu'on désigne par $z$ un entier quelconque, on aura en général $x = \alpha + \theta z$, et ainsi les valeurs de $x$ qui rendent $Ax + B$ divisible par $\theta$, forment elles-mêmes une progression arithmétique $\alpha, \alpha + \theta, \alpha + 2\theta$ &c., dont la différence est $\theta$.

Il suit de-là que sur $\theta$ termes consécutifs pris par-tout où l'on voudra dans la suite $-A+B$, $B$, $A+B$, $2A+B$, &c., il y en aura nécessairement un divisible par $\theta$. En général, les termes divisibles par $\theta$, dans la suite dont il s'agit, seront placés à la même distance les uns des autres, et cette distance comprendra toujours un nombre de termes $\theta$.

XXI. Supposons que la série commence au terme $A + B$ lorsque $x = 1$; si on considère $n$ termes consécutifs à compter du premier, et que de ces $n$ termes on retranche tous ceux qui sont divisibles par $\theta$, il restera $n\left(1-\frac{1}{\theta}\right)$ termes non-divisibles par $\theta$.

Dans les applications de cette formule, le résultat sera toujours exact, tant que $n$ sera un multiple $\theta$. Mais $n$ peut être un nombre quelconque non divisible par $\theta$, et alors la quantité $n\left(1-\frac{1}{\theta}\right)$ contiendra un entier $\alpha$ plus un reste $\frac{c}{\theta}$. L'entier $\alpha$ a une signification non-équivoque; quant à la fraction $\frac{c}{\theta}$, elle tient lieu tantôt de zéro; tantôt de l'unité, suivant les différens cas. Cette fraction exprime en quelque sorte la probabilité que le nombre des termes non-divisibles par $\theta$ sera $\alpha + 1$; mais il peut être $\alpha$ seulement.

---

(1) Car en faisant successivement $x = 0, 1, 2, \ldots \theta - 1$, les restes de la division de $Ax + B$ par $\theta$ doivent être différens les uns des autres, et plus petits que $\theta$. Donc il y en a un qui sera zéro. Deux restes ne peuvent pas être les mêmes, car si $Am + B$ et $An + B$ donnoient le même reste, il faudroit que leur différence $A(m-n)$ fût divisible par $\theta$; ce qui n'a pas lieu, puisque $A$ n'est pas divisible par $\theta$, non plus que $m-n$, qui est $< \theta$.

XXII. Si $\omega$ est un nombre premier non-diviseur de $A$, on trouvera semblablement que dans la suite finie

$$A+B,\ 2A+B,\ 3A+B \ldots\ldots nA+B$$

il y a $n\left(1-\frac{1}{\omega}\right)$ termes non-divisibles par $\omega$, et la fraction qui peut être contenue dans $n\left(1-\frac{1}{\omega}\right)$ tiendra lieu suivant les différens cas de 0 ou de 1.

Donc si on veut savoir combien dans la même suite il y a de termes qui ne sont divisibles ni par $\omega$ ni par $\theta$, on trouvera que ce nombre est $n\left(1-\frac{1}{\theta}\right)\left(1-\frac{1}{\omega}\right)$. En effet, si l'on suppose, pour plus de simplicité, que $n$ est multiple de $\omega\theta$, et qu'on fasse en conséquence $n=n'\omega\theta$, on pourra distinguer dans $n$ quatre sortes de termes, 1°. les $N$ termes qui ne sont divisibles ni par $\theta$ ni par $\omega$; 2°. les $n'\omega$ termes qui sont divisibles par $\theta$; 3°. les $n'\theta$ termes qui sont divisibles par $\omega$; 4°. les $n'$ termes qui sont divisibles par $\omega\theta$. Or il est évident que ceux-ci sont compris deux fois dans les termes $n'\omega+n'\theta$, et qu'ainsi en réunissant tous les termes distincts, on aura $n=N+n'\omega+n'\theta-n'$; d'où résulte

$$N=n\left(1-\frac{1}{\theta}-\frac{1}{\omega}+\frac{1}{\theta\omega}\right)=n\left(1-\frac{1}{\theta}\right)\left(1-\frac{1}{\omega}\right).$$

Formule qui sera rigoureusement vraie, si $n$ est un multiple de $\omega\theta$, et qui approchera de la vérité dans tous les autres cas, de manière que l'erreur ne pourra jamais être de deux unités.

XXIII. Par un raisonnement semblable, on prouvera que si $\theta$, $\lambda$, $\mu$, $\nu$, &c. sont des nombres premiers quelconques non-diviseurs de $A$, la formule

$$n\left(1-\frac{1}{\theta}\right)\left(1-\frac{1}{\lambda}\right)\left(1-\frac{1}{\mu}\right)\left(1-\frac{1}{\nu}\right)\ \&c.$$

représentera le nombre de termes de la suite $A+B, 2A+B \ldots nA+B$ qui ne sont divisibles par aucun des nombres premiers $\theta, \lambda, \mu, \nu$, &c. Cette formule pourra, dans les cas particuliers, s'écarter quelque peu de la vérité à raison des fractions introduites par chaque dé-

nominateur, mais l'erreur ne pourra jamais s'élever à autant d'unités qu'il y a de dénominateurs.

XXIV. Si $A$ et $B$ avoient un diviseur commun, il est clair que la formule $Ax+B$ ne pourroit contenir aucun nombre premier (si ce n'est peut-être le diviseur dont il s'agit).

Supposons donc que $A$ et $B$ sont premiers entr'eux; et parce qu'alors la formule $Ax+B$ peut représenter divers nombres premiers, cherchons combien il y a de ces nombres dans la progression $A+B$; $2A+B \ldots\ldots nA+B$.

D'après la formule précédente, il faudra former le produit

$$n\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{5}{7}\cdot\ldots\ldots\frac{\omega-1}{\omega}$$

dans lequel on fera entrer tous les nombres premiers 3, 5, 7 jusqu'au plus grand $\omega$ compris dans $\sqrt{(nA+B)}$, en exceptant seulement ceux qui divisent $A$.

Cela posé, si $A+B$ est plus grand que $\sqrt{(nA+B)}$, la formule précédente sera le nombre demandé.

Mais si $A+B$ est plus petit que $\sqrt{(nA+B)}$, il faudra ajouter à cette formule autant d'unités qu'il y a de nombres premiers moindres que $\sqrt{(nA+B)}$ dans la suite proposée

$$A+B,\ 2A+B\ldots\ldots nA+B.$$

XXV. Veut-on savoir, par exemple, combien il y a de nombres premiers dans les 1000 premiers termes de la suite

49, 109, 169, 229, 289, 349, &c.

dont le terme général est $60x-11$ ? Le millième terme est 59989, sa racine quarrée 244, et le nombre premier prochainement moindre 241; d'ailleurs 60 est divisible par 3 et par 5; donc il faut prendre pour diviseurs tous les nombres premiers depuis 7 jusqu'à 241 inclusivement, ce qui donnera pour l'expression du nombre demandé

$$1000\left(\frac{6}{7}\cdot\frac{10}{11}\cdot\frac{12}{13}\cdot\frac{16}{17}\cdot\frac{18}{19}\cdot\frac{22}{23}\cdot\ldots\ldots\frac{240}{241}\right)+2.$$

J'ajoute 2 unités, parce qu'il y a dans les premiers termes de la suite deux nombres premiers 109 et 229 moindres que 241.

XXVI. Pour achever ce calcul, et en général, pour trouver combien il y a de nombres premiers dans $n$ termes successifs d'une progression arithmétique donnée ($n$ étant assez considérable pour que les petites aberrations produites par les fractions, en plus ou en moins, ne soient pas sensibles), il seroit nécessaire d'avoir une table des valeurs du produit $\frac{2}{3}.\frac{4}{5}.\frac{6}{7}.\frac{10}{11}\ldots$ &c. formé avec la suite des nombres premiers, et borné successivement à chacun de ces nombres. Voici un essai de cette table.

VALEURS

VALEURS successives du produit $\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{6}{7}\cdots\cdots\frac{\omega-1}{\omega}$ continué jusqu'au nombre premier $\omega$.

| NOMBRE $\omega$. | PRODUIT. | NOMBRE $\omega$. | PRODUIT. |
|---|---|---|---|
| 3 | 0, 666 667 | 157 | 0, 218 316 |
| 5 | 0, 533 333 | 163 | 0, 216 977 |
| 7 | 0, 457 143 | 167 | 0, 215 678 |
| 11 | 0, 415 584 | 173 | 0, 214 431 |
| 13 | 0, 383 616 | 179 | 0, 213 233 |
| 17 | 0, 361 051 | 181 | 0, 212 055 |
| 19 | 0, 342 048 | 191 | 0, 210 941 |
| 23 | 0, 327 176 | 193 | 0, 209 848 |
| 29 | 0, 315 894 | 197 | 0, 208 783 |
| 31 | 0, 305 704 | 199 | 0, 207 734 |
| 37 | 0, 297 442 | 211 | 0, 206 749 |
| 41 | 0, 290 187 | 223 | 0, 205 822 |
| 43 | 0, 283 439 | 227 | 0, 204 915 |
| 47 | 0, 277 407 | 229 | 0, 204 020 |
| 53 | 0, 272 183 | 233 | 0, 203 144 |
| 59 | 0, 267 570 | 239 | 0, 202 294 |
| 61 | 0, 263 111 | 241 | 0, 201 455 |
| 67 | 0, 259 184 | 251 | 0, 200 652 |
| 71 | 0, 255 534 | 257 | 0, 199 871 |
| 73 | 0, 252 033 | 263 | 0, 199 111 |
| 79 | 0, 248 843 | 269 | 0, 198 371 |
| 83 | 0, 245 845 | 271 | 0, 197 639 |
| 89 | 0, 243 083 | 277 | 0, 196 925 |
| 97 | 0, 240 577 | 281 | 0, 196 224 |
| 101 | 0, 238 195 | 283 | 0, 195 531 |
| 103 | 0, 235 882 | 293 | 0, 194 864 |
| 107 | 0, 233 677 | 307 | 0, 194 229 |
| 109 | 0, 231 533 | 311 | 0, 193 605 |
| 113 | 0, 229 484 | 313 | 0, 192 986 |
| 127 | 0, 227 677 | 317 | 0, 192 377 |
| 131 | 0, 225 939 | 331 | 0, 191 796 |
| 137 | 0, 224 290 | 337 | 0, 191 227 |
| 139 | 0, 222 676 | 347 | 0, 190 676 |
| 149 | 0, 221 181 | 349 | 0, 190 130 |
| 151 | 0, 219 716 | 353 | 0, 189 591 |

XXVII. Au moyen de cette table, on trouvera facilement la valeur du produit $\frac{6}{7}.\frac{10}{11}.\frac{12}{13}\ldots\ldots\frac{240}{241}$ dont on a eu besoin dans le problême du n°. XXV, car ce produit n'est autre chose, aux deux premiers facteurs près, que celui qui est donné dans la table vis-à-vis de 241 ; de sorte que le produit dont il s'agit $=\frac{15}{8}\times 0,201\,455=0,377\,728$. De-là résulte le nombre demandé $377,7+2$, ou à-peu-près 380, c'est-à-dire qu'il y a environ 380 nombres premiers compris dans les 1000 premiers termes de la suite arithmétique 49, 109, 169, &c.

XXVIII. Supposons encore qu'on cherche combien il y a de nombres premiers au-dessous de 100000. Pour cela, il faut considérer les 50000 premiers termes de la suite 1, 3, 5.... 99999; or la racine de 99999 est à-peu-près 316, et le nombre premier, prochainement ~~moindre, est 313; on aura~~ donc, au moyen de la table, le produit $500\,000.\frac{2}{3}.\frac{4}{5}\ldots\frac{312}{313}=500\,000\times 0,192\,986=9649$; à quoi ajoutant 66, parce que 313 est le 66e des nombres premiers (2 compris) on aura 9715 pour le nombre demandé des nombres premiers au-dessous de 100 000. L'erreur, dans ce résultat, ne peut s'élever à 66; ce qui fait à peine la 146e partie du total.

XXIX. Si on cherchoit combien il y a de nombres premiers au-dessous de 1000, on trouveroit par les mêmes procédés, que le nombre est environ 165 (il est réellement 170, l'aberration étant causée par les fractions).

On voit par-là, que jusqu'à 1000 les nombres premiers composent la sixième partie de tous les nombres; mais à 100000 ils ne composent plus que la dixième partie (1) : on conçoit en même tems

(1) S'il y a $b$ nombres premiers compris dans la progression naturelle 1,2,3,4,5. . $a$, il est remarquable que suivant les diverses valeurs de $a$, on ait à très-peu-près les rapports suivans :

$$a=10^1,\quad 10^2,\quad 10^3,\quad 10^4,\quad 10^5\ldots\ldots$$

$$\frac{b}{a}=\frac{1}{2},\quad \frac{1}{4},\quad \frac{1}{6},\quad \frac{1}{8},\quad \frac{1}{10}\ldots\ldots$$

D'où il paroît qu'on peut conclure en général $b=\frac{a}{2\,\mathrm{l}\,a}$, l $a$ désignant le logarithme

qu'à 1000000 la proportion sera encore moindre et ainsi de suite. En effet, la probabilité qu'un nombre pris au hasard sera premier, est d'autant moindre que ce nombre est plus grand ; car plus le nombre est grand, plus il y a de divisions à essayer pour s'assurer si le nombre est premier ou s'il ne l'est pas.

XXX. Nous remarquerons encore, que si on considère les seize suites dont les termes généraux sont : $60x+1$, $60x-1$, $60x+7$, $60x-7$, $60x+11$, $60x-11$, &c. (art. XV), et qu'on cherche, par exemple, combien il y a de nombres premiers dans un million des premiers termes de chaque suite, on trouveroit sensiblement le même nombre pour chacune ; d'où il suit que tous les nombres premiers (sauf 2, 3 et 5) sont répartis également entre ces différentes suites, et que chacune peut être censée contenir la seizième partie de la totalité des nombres premiers.

---

de $a$ pris dans les tables ordinaires ; cette formule très-simple peut être regardée comme suffisamment approchée, au moins lorsque $a$ n'excède pas 1000000. Ainsi si on demande combien il y a de nombres premiers depuis 1 jusqu'à 400000, on trouvera que ce nombre est $\frac{400000}{2\times 5,602}$ ou 35700 à-peu-près.

Au reste, il est vraisemblable que la formule rigoureuse qui donne la valeur de $b$ lorsque $a$ est très-grand, est de la forme $b=\frac{a}{A\log. a+B}$, $A$ et $B$ étant des coefficiens constans, et log. $a$ désignant un logarithme hyperbolique. La détermination exacte de ces coefficiens seroit un problême curieux et digne d'exercer la sagacité des Analystes.

# TABLE

des nombres premiers au-dessous de 1000.

| | |
|---|---|
| 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97 .............. | 26 |
| 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199 .... | 47 |
| 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293. .......................... | 63 |
| 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397 .............................. | 79 |
| 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499 ...................... | 96 |
| 503, 509, 521, 523, 527, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599 ................................ | 111 |
| 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691 ........................... | 127 |
| 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797 ................................... | 141 |
| 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887 ................................ | 156 |
| 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997 ..................................... | 170 |

# PREMIÈRE PARTIE.

## EXPOSITION DE DIVERSES MÉTHODES ET PROPOSITIONS RELATIVES A L'ANALYSE INDÉTERMINÉE.

### §. I. *Des Fractions continues.*

(1) Pour changer une quantité quelconque $x$ rationnelle ou irrationnelle en fraction continue, le principe est de faire successivement

$$x = \alpha + \frac{1}{x'}, \quad x' = \alpha' + \frac{1}{x''}, \quad x'' = \alpha'' + \frac{1}{x'''}, \quad \&c.$$

$\alpha$ étant le plus grand entier contenu dans $x$, $\alpha'$ le plus grand entier contenu dans $x'$, et ainsi de suite. De cette manière, il est visible que la quantité $x$ sera transformée en cette fraction continue

$$\alpha + \frac{1}{\alpha' + \frac{1}{\alpha'' + \frac{1}{\alpha''' + \&c.}}}$$

laquelle aura un nombre fini ou infini de termes, selon que la quantité $x$ est rationnelle ou irrationnelle.

Ces termes ou *quotiens* $\alpha$, $\alpha'$, $\alpha''$, &c. sont supposés, ainsi que la quantité $x$, toujours positifs (le premier $\alpha$ seroit zéro, si $x$ étoit au-dessous de l'unité). Quelquefois cependant il convient, pour rendre la suite plus convergente, d'admettre des quotiens négatifs; mais c'est une exception dont il faut avertir expressément, et qui n'aura pas lieu dans ce qui suit.

(2) Lorsque la quantité $x$ est une fraction rationnelle $\frac{M}{N}$, pour transformer cette quantité en fraction continue, il ne s'agit que de faire, sur les deux nombres $M$ et $N$, la même opération que

si on en cherchoit le plus grand commun diviseur. Voici le type de cette opération, en supposant $M > N$.

$$\text{reste}\ \frac{M}{P}\left\{\frac{N}{\alpha}\right.,\qquad \text{reste}\ \frac{N}{Q}\left\{\frac{P}{\alpha'}\right.,\qquad \text{reste}\ \frac{P}{R}\left\{\frac{Q}{\alpha''}\right.,\qquad \&c.$$

Par ce moyen, on a successivement

$$\frac{M}{N} = \alpha + \frac{P}{N},\quad \frac{N}{P} = \alpha' + \frac{Q}{P},\quad \frac{P}{Q} = \alpha'' + \frac{R}{Q},\quad \&c.$$

Donc

$$\frac{M}{N} = \alpha + \cfrac{1}{\alpha' + \cfrac{1}{\alpha'' + \&c.}}\qquad \text{et}\ \frac{N}{M} = \cfrac{1}{\alpha + \cfrac{1}{\alpha' + \cfrac{1}{\alpha'' + \&c.}}}$$

Dans ce cas, les termes de la fraction continue ne sont autre chose que les quotiens successivement trouvés par l'opération du commun diviseur, ~~et il est clair que~~ la fraction continue sera toujours bornée à un certain nombre de termes qui pourra être plus ou moins grand, selon que la fraction $\frac{M}{N}$ sera plus ou moins composée.

(3) Nous avons appelé *quotiens* les termes successifs $\alpha, \alpha', \alpha''$, &c. de la fraction *continue*; nous appellerons semblablement *quotiens-complets* les quantités $x, x', x''$, &c. résultantes de l'opération du développement, et dont les entiers $\alpha, \alpha', \alpha''$, &c. font la plus grande partie. Chaque quotient-complet renferme implicitement, outre l'entier qui y est contenu, tous les quotiens suivans de la fraction continue, puisque c'est par le développement de ce quotient-complet qu'on trouve successivement tous les quotiens suivans.

Si on a une expression algébrique qui représente la valeur de la fraction continue prolongée jusqu'au terme $\alpha^{(n)}$ inclusivement, et que dans cette expression on substitue, au lieu de $\alpha^{(n)}$, le quotient-complet $x^{(n)}$, il est clair que le résultat sera la valeur exacte de $x$; car quand même la fraction continue s'étendroit à l'infini, on auroit rigoureusement

$$x = \alpha + \frac{1}{x'},\qquad x = \alpha + \cfrac{1}{\alpha' + \cfrac{1}{x''}},\qquad x = \alpha + \cfrac{1}{\alpha' + \cfrac{1}{\alpha'' + \cfrac{1}{x'''}}},\qquad \&c.$$

De-là il suit qu'au moyen de chaque quotient-complet, on peut toujours reproduire la valeur entière et exacte de la quantité développée, quelque loin qu'on ait poussé le développement. Cette propriété recevra par la suite un grand nombre d'applications utiles.

(4) Étant proposée une fraction continue

$$x = \alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \cfrac{1}{\delta + \text{\&c.}}}}$$

pour la réduire en fraction ordinaire, ou pour en trouver la valeur, quel que soit le nombre de ses termes, il faut observer la loi que suivent les résultats obtenus, en prenant successivement le premier terme, les deux premiers, les trois premiers, &c. de cette quantité; or on a, par les réductions ordinaires:

$$\alpha = \frac{\alpha}{1}, \quad \alpha + \frac{1}{\beta} = \frac{\alpha\beta + 1}{\beta}, \quad \alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma}} = \frac{\alpha\beta\gamma + \gamma + \alpha}{\beta\gamma + 1}$$

$$\alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \cfrac{1}{\delta}}} = \frac{\alpha\beta\gamma\delta + \gamma\delta + \alpha\delta + \alpha\beta + 1}{\beta\gamma\delta + \delta + \beta}, \quad \text{\&c.}$$

De-là il suit que $\frac{m}{n}, \frac{p}{q}$ étant deux résultats consécutifs, et $\mu$ un nouveau quotient, le résultat suivant sera $\frac{p\mu + m}{q\mu + n}$; c'est la loi générale suivant laquelle on peut calculer facilement la valeur de la fraction continue proposée, quel que soit le nombre de ses termes. Voici le type de l'opération:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Quotiens ...... | | $\alpha$, | $\beta$, | $\gamma$, | $\delta$, | ... $\mu$, | $\mu'$, | $\mu''$ ... | &c. |
| Fractions convergentes | .. $\frac{1}{0}$, | $\frac{\alpha}{1}$, | $\frac{\alpha\beta + 1}{\beta}$, | $\frac{\alpha\beta\gamma + \gamma + \alpha}{\beta\gamma + 1}$ | ... | $\frac{p}{q}$, | $\frac{p'}{q'}$, | $\frac{p''}{q''}$ ... | &c. |

Sur une ligne on écrit les quotiens successifs $\alpha$, $\beta$, $\gamma$, $\delta$, &c.; au-dessous des deux premiers on met les deux fractions $\frac{1}{0}, \frac{\alpha}{1}$ (la première étant mise seulement pour mieux faire sentir la loi), ensuite on multiplie chaque numérateur par le quotient écrit au-

dessus, on ajoute le numérateur précédent, et la somme est le numérateur suivant; on fait de même à l'égard des dénominateurs, et la suite des fractions qui résultent de ce calcul représente les diverses valeurs de la fraction continue proposée, selon qu'on en prend plus ou moins de termes. Ces valeurs doivent approcher de plus en plus de la valeur totale de la fraction continue, c'est pourquoi nous les appelons *fractions convergentes;* si la fraction continue ne s'étend pas à l'infini, la dernière des fractions convergentes sera la valeur exacte de la fraction continue proposée.

(5) Pour rendre raison de la loi que nous venons d'indiquer, supposons qu'elle ait été vérifiée au moins jusqu'à un certain quotient $\mu$; soit $\frac{p}{q}$ la fraction convergente qui répond au quotient $\mu$, ou qui est placée immédiatement au-dessous; soient en même tems $\frac{p^{\circ}}{q^{\circ}}$ la fraction convergente qui précède $\frac{p}{q}$, et $\frac{p'}{q'}$ celle qui la suit en cette sorte.......................... $\frac{p^{\circ}}{q^{\circ}}, \overset{\mu}{\frac{p}{q}}, \frac{p'}{q'}$.
on aura, suivant la loi dont il s'agit:

$$p' = p\mu + p^{\circ}$$
$$q' = q\mu + q^{\circ}$$

et la fraction $\frac{p'}{q'}$ sera celle qui résulte de tous les quotiens de la fraction continue jusqu'à $\mu$ inclusivement. Ajoutons maintenant un nouveau quotient $\mu'$ à la suite de $\mu$, et soit $\frac{p''}{q''}$ la valeur de la fraction continue calculée jusqu'au quotient $\mu'$ inclusivement, il est clair que la valeur analytique de $\frac{p''}{q''}$ ne sera autre chose que celle de $\frac{p'}{q'}$ dans laquelle, au lieu de $\mu$, on mettroit $\mu + \frac{1}{\mu'}$; donc on aura

$$\frac{p''}{q''} = \frac{p\left(\mu + \frac{1}{\mu'}\right) + p^{\circ}}{q\left(\mu + \frac{1}{\mu'}\right) + q^{\circ}} = \frac{p'\mu' + p}{q'\mu' + q}$$

Donc

Donc la fraction convergente $\frac{p''}{q''}$ se déduira des deux précédentes $\frac{p}{q}, \frac{p'}{q'}$, et du quotient $\mu'$ répondant à la dernière, suivant la loi

$$p'' = p'\mu' + p$$
$$q'' = q'\mu' + q.$$

Et ainsi cette loi de continuation aura lieu généralement dans toute l'étendue de la fraction continue.

(6) Il est à remarquer que les fractions convergentes successives $\frac{1}{0}$, $\frac{\alpha}{1}$, $\frac{\alpha\beta + 1}{\beta}$, $\frac{\alpha\beta\gamma + \gamma + \alpha}{\beta\gamma + 1}$, &c. sont alternativement plus grandes et plus petites que la valeur totale $x$ de la fraction continue; c'est une suite de ce que les quotiens $\alpha$, $\beta$, $\gamma$, $\delta$, &c. sont supposés tous positifs. En effet, si on prend un seul terme $\alpha$, on a évidemment $\alpha < x$; si on en prend deux, on aura $\alpha + \frac{1}{\beta} > x$; car pour avoir la vraie valeur de $x$, il faudroit augmenter le dénominateur $\beta$ d'une certaine quantité. On verra de même, qu'en prenant trois termes $\alpha + \frac{1}{\beta + \frac{1}{\gamma}}$, le résultat est plus petit que $x$, et ainsi alternativement.

Donc *la valeur de* **x** *est toujours comprise entre deux fractions convergentes consécutives.*

Cela posé, je dis que si $\frac{p^\circ}{q^\circ}$, $\frac{p}{q}$ sont deux fractions convergentes consécutives, on aura $pq^\circ - p^\circ q = \pm 1$, savoir $+1$ si la fraction $\frac{p}{q}$ est du nombre des fractions plus grandes que $x$, ou si elle est de rang impair ($\frac{1}{0}$ étant censée la première), et $-1$ si elle est de rang pair.

En effet, si l'on considère trois fractions convergentes consécutives $\frac{p^\circ}{q^\circ}$, $\frac{p}{q}$, $\frac{p'}{q'}$, et que $\mu$ soit le quotient qui répond à $\frac{p}{q}$, on aura, suivant la loi démontrée, $p' = \mu p + p^\circ$, $q' = \mu q + q^\circ$; d'où résulte $p'q - pq' = -(pq^\circ - p^\circ q)$. Mais par la même raison, si la

fraction $\frac{p^\circ}{q^\circ}$ est précédée de $\frac{p^{\circ\circ}}{q^{\circ\circ}}$, on aura $pq^\circ - p^\circ q = -(p^\circ q^{\circ\circ} - p^{\circ\circ} q^\circ)$. Remontant ainsi jusqu'aux deux premières fractions $\frac{1}{0}$, $\frac{\alpha}{1}$, où la différence analogue $1 \times 1 - \alpha \times 0 = 1$, on en conclura que la différence $pq^\circ - p^\circ q$ est toujours égale à l'unité avec le signe $+$, si $\frac{p}{q}$ est de rang impair, et le signe $-$ dans le cas contraire.

(7) Cherchons présentement quelle est la différence entre une fraction convergente $\frac{p}{q}$ et la valeur entière $x$ de la fraction continue. Pour cela, soit toujours $\frac{p^\circ}{q^\circ}$ la fraction convergente qui précède $\frac{p}{q}$, et $y$ le quotient-complet qui répond à celle-ci, on aura, suivant ce qui a été démontré, $x = \frac{py + p^\circ}{qy + q^\circ}$, d'où l'on tire

$$x - \frac{p}{q} = \frac{p^\circ q - pq^\circ}{q(qy + q^\circ)} = \frac{\mp 1}{q(qy + q^\circ)}$$

$$\text{et } x - \frac{p^\circ}{q^\circ} = \frac{(pq^\circ - p^\circ q)y}{q^\circ(qy + q^\circ)} = \frac{\pm y}{q^\circ(qy + q^\circ)}.$$

De-là on voit 1°. que $x - \frac{p}{q}$ et $x - \frac{p^\circ}{q^\circ}$ sont toujours de signes contraires, et qu'ainsi la valeur exacte de $x$ est toujours comprise entre deux fractions convergentes consécutives.

2°. Que la différence $x - \frac{p}{q}$ est en général moindre que $\frac{1}{q^2}$, et par conséquent peut être représentée par $\frac{\pm \delta}{q^2}$, $\delta$ étant plus petite que l'unité.

3°. Que la quantité $p - qx$ est plus petite (abstraction faite de son signe) que $p^\circ - q^\circ x$. Car on a $\frac{1}{y} = \frac{p - qx}{q^\circ x - p^\circ}$; or par la nature des fractions continues, $y$ est toujours plus grand que l'unité. Donc à plus forte raison, $\frac{p}{q} - x$ est plus petit que $\frac{p^\circ}{q^\circ} - x$; donc

*chaque fraction convergente* $\frac{p}{q}$ *est plus approchée de* $x$ *que toutes celles qui la précèdent.* Propriété qui justifie la dénomination de ces fractions.

(8) Soit maintenant $\frac{\pi}{\varphi}$ une fraction quelconque dont le dénominateur $\varphi$ soit moindre que $q$; je dis que la quantité $\pi - \varphi x$, abstraction faite de son signe, sera plus grande que $p - qx$ et même que $p^\circ - q^\circ x$.

Car si l'on prend $M = p\varphi - q\pi$, $N = p^\circ\varphi - q^\circ\pi$, on aura réciproquement,

$$(pq^\circ - p^\circ q)\pi = p^\circ M - pN$$
$$(pq^\circ - p^\circ q)\varphi = q^\circ M - qN.$$

Or on suppose $\varphi < q$, et on a $pq^\circ - p^\circ q = \pm 1$; donc les nombres $M$ et $N$ seront nécessairement de même signe. Cela posé, on aura $(pq^\circ - p^\circ q)(\pi - \varphi x) = M(p^\circ - q^\circ x) - N(p - qx)$. Mais $M$ et $N$ sont de même signe, les quantités $p^\circ - q^\circ x$, $p - qx$ sont de signes contraires; et on a d'ailleurs $pq^\circ - p^\circ q = \pm 1$; donc $\pi - \varphi x$ est non-seulement plus grande que chacune des quantités $p^\circ - q^\circ x$, $p - qx$; mais elle est au moins égale à leur somme.

Puisque $\varphi$ étant supposé $< q$, on a généralement $\pi - \varphi x > p - qx$, il s'ensuit, à plus forte raison, qu'on a $\frac{\pi}{\varphi} - x > \frac{p}{q} - x$; donc la fraction convergente $\frac{p}{q}$ est toujours plus approchée de $x$ que ne l'est toute autre fraction $\frac{\pi}{\varphi}$ dont le dénominateur est moindre que $q$.

Cette propriété des fractions continues s'applique avec avantage, toutes les fois qu'il est question d'exprimer par des rapports les plus simples et les plus approchés qu'il est possible, des rapports entre de très-grands nombres, ou des nombres irrationnels.

(9) Étant donnée une fraction $\frac{p}{q}$ dont la différence avec une quantité quelconque $x$ est $\pm \frac{\delta}{q^2}$, $\delta$ étant plus petit que l'unité, on

demande quelle est la condition pour que la fraction $\frac{p}{q}$ soit l'une des fractions convergentes données par le développement de $x$ en fraction continue.

Pour cela, supposons que le développement de la fraction $\frac{p}{q}$ produise les quotiens successifs $\alpha$, $\beta$, $\gamma \ldots\ldots \mu$, au moyen desquels on calculera les fractions convergentes vers $\frac{p}{q}$, comme il suit :

| | | | | | |
|---|---|---|---|---|---|
| Quotiens............. | $\alpha$ , | $\beta$ , | $\gamma$ ............ | | $\mu$ |
| Fract. converg........ | $\frac{1}{0}$ , | $\frac{\alpha}{1}$ , | $\frac{\alpha\beta+1}{\beta}$....... | $\frac{p^\circ}{q^\circ}$ , | $\frac{p}{q}$. |

Si la fraction $\frac{p}{q}$ est une fraction convergente vers $x$, il faudra que les quotiens $\alpha$, $\beta$, $\gamma \ldots\ldots \mu$ naissent également du développement de $x$, et que le quotient $\mu$ soit suivi de plusieurs autres $\mu'$, $\mu''$, &c. Appelons $y$ le quotient-complet qui, dans le développement de $x$, répond à la fraction convergente $\frac{p}{q}$, on aura $x = \frac{py + p^\circ}{qy + q^\circ}$, d'où résulte

$$x - \frac{p}{q} = \frac{p^\circ q - p q^\circ}{q(qy + q^\circ)} = \frac{\pm 1}{q(qy + q^\circ)}.$$

Cette quantité doit être égalée à $\frac{\pm \delta}{q^2}$, ainsi il faut d'abord que le signe de $p q^\circ - p q^\circ$ soit le même que celui de $\delta$. Or c'est ce qu'il est toujours possible d'obtenir.

En effet, la suite des quotiens $\alpha$, $\beta \ldots\ldots \mu$ étant tirée de la fraction donnée $\frac{p}{q}$, par la même opération qui serviroit à trouver le commun diviseur de $p$ et $q$, le dernier de ces quotiens $\mu$ est toujours plus grand que l'unité. Car s'il étoit égal à l'unité, la fraction continue $\alpha + \frac{1}{\beta + \&c.}$, au lieu d'être terminée par les deux termes $\frac{1}{\lambda + \frac{1}{\mu}}$, le seroit par le seul terme $\frac{1}{\lambda + 1}$. Réciproquement donc

on pourra, si on le juge à propos, étendre le dernier quotient $\mu$ en deux autres $\mu-1$, $1$; de sorte que le calcul des fractions convergentes vers $\frac{p}{q}$ pourra être terminé à volonté de l'une ou de l'autre de ces deux manières :

$$\ldots \lambda,\ \mu \qquad\qquad \ldots\ \lambda,\ \mu-1,\ 1$$
$$\ldots \frac{m}{n},\ \frac{p}{q} \qquad\qquad \frac{m}{n},\ \frac{p-m}{q-n},\ \frac{p}{q}.$$

Soit $\frac{p^\circ}{q^\circ}$ la fraction convergente qui dans l'une ou l'autre hypothèse précède $\frac{p}{q}$, on pourra donc prendre ou $p^\circ=m$, $q^\circ=n$, ou $p^\circ=p-m$, $q^\circ=q-n$; mais le signe de $pq^\circ-p^\circ q$ est le contraire dans un cas de ce qu'il est dans l'autre; donc en effet on peut toujours faire en sorte que la quantité $pq^\circ-p^\circ q$ ait le signe qu'on voudra.

On aura donc sans ambiguité $\frac{1}{q(qy+q^\circ)}=\frac{\delta}{q^2}$, ou $\delta=\frac{q}{qy+q^\circ}$. Or il faut que $y$ soit positif et plus grand que l'unité, pour que $y$ soit le quotient-complet qui répond à la fraction convergente $\frac{p}{q}$, donc on aura $\delta<\frac{q}{q+q^\circ}$; et réciproquement si on a $\delta<\frac{q}{q+q^\circ}$, la valeur de $y$ sera positive et plus grande que l'unité, donc $\frac{p}{q}$ sera l'une des fractions convergentes vers $x$. C'est la condition qu'il s'agissoit de trouver.

Cette condition seroit remplie entr'autres cas, si on avoit $\delta<\frac{1}{2}$, parce que $q^\circ$ est toujours $<q$.

(10) Nous placerons ici une application de la propriété précédente, laquelle sera utile dans la résolution des équations indéterminées du second degré.

Soit $p^2-Aq^2=\pm D$ une équation indéterminée dans laquelle $D$ est $<\sqrt{A}$, je dis que si cette équation est résoluble, la fraction $\frac{p}{q}$ sera comprise parmi les fractions convergentes vers $\sqrt{A}$.

En effet, de cette équation on tire $p-q\sqrt{A}=\frac{\pm D}{p+q\sqrt{A}}$, et ainsi $\frac{p}{q}-\sqrt{A}$ que je représente par $\frac{\pm\delta}{q^2}=\frac{\pm D}{q(p+q\sqrt{A})}$, donc $\delta=\frac{Dq}{p+q\sqrt{A}}$; soit $\frac{p^\circ}{q^\circ}$ la fraction convergente qui précède $\frac{p}{q}$ et qui est déterminée de manière que le signe de $\delta$ soit le même que celui de $D$, il restera à prouver qu'on a $\frac{Dq}{p+q\sqrt{A}}<\frac{q}{q+q^\circ}$, ou $D(q+q^\circ)<p+q\sqrt{A}$. Dans le second membre, je mets, au lieu de $p$, sa valeur $q\sqrt{A}\pm\frac{\delta}{q}$, et l'inégalité à prouver pourra s'écrire ainsi:

$$(q+q^\circ)(\sqrt{A}-D)+(q-q^\circ)\sqrt{A}\pm\frac{\delta}{q}>0.$$

Or cette inégalité est manifeste, puisqu'on a $\sqrt{A}>D$, $q>q^\circ$, et que la partie seule $(q-q^\circ)\sqrt{A}$, qui est au moins égale à $\sqrt{A}$, surpasse $\frac{\delta}{q}$ qui est plus petit que l'unité. Donc $\frac{p}{q}$ sera toujours comprise parmi les fractions convergentes vers $\sqrt{A}$, de sorte qu'il ne s'agit que de développer $\sqrt{A}$ en fraction continue, et de calculer les fractions convergentes qui en résultent, pour avoir toutes les solutions en nombres entiers de l'équation $x^2-Ay^2=\pm D$, $D$ étant $<\sqrt{A}$.

(11) Considérons une fraction continne plus petite que l'unité, et d'un nombre fini de termes $\frac{1}{\alpha+\frac{1}{\beta+\&c.}}=\frac{p}{q}$; le calcul des fractions convergentes étant fait à l'ordinaire, comme il suit:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Quotiens ........ | $\alpha$, | $\beta$, | $\gamma$ ....... | | $\varkappa$, | $\lambda$, | $\mu$ | |
| Fract. converg.... | $\frac{0}{1}$, | $\frac{1}{\alpha}$, | $\frac{\beta}{\alpha\beta+1}$ ..... | $\frac{p^{\circ\circ\circ}}{q^{\circ\circ\circ}}$, | $\frac{p^{\circ\circ}}{q^{\circ\circ}}$, | $\frac{p^\circ}{q^\circ}$, | $\frac{p}{q}$ | |

on aura, suivant la loi de formation:

$$q = \mu q^{\circ} + q^{\circ\circ} \quad \text{partant} \quad \frac{q^{\circ}}{q} = \frac{1}{\mu + \frac{q^{\circ\circ}}{q^{\circ}}}$$

$$q^{\circ} = \lambda q^{\circ\circ} + q^{\circ\circ\circ} \qquad \frac{q^{\circ\circ}}{q^{\circ}} = \frac{1}{\lambda + \frac{q^{\circ\circ\circ}}{q^{\circ\circ}}}$$

$$q^{\circ\circ} = \kappa q^{\circ\circ\circ} + q^{\circ\circ\circ\circ} \qquad \frac{q^{\circ\circ\circ}}{q^{\circ\circ}} = \frac{1}{\kappa + \frac{q^{\circ\circ\circ\circ}}{q^{\circ\circ\circ}}}$$

&c. &c.

Donc en général,

$$\frac{q^{\circ}}{q} = \frac{1}{\mu + \frac{1}{\lambda + \frac{1}{\kappa \ldots + \frac{1}{\alpha}}}}$$

C'est-à-dire que le développement de $\frac{q^{\circ}}{q}$ donne les quotiens $\mu, \lambda, \kappa, \ldots \; \beta, \alpha$ qui ne sont autre chose que les termes de la fraction continue proposée, pris dans l'ordre inverse.

Donc s'il arrive que ces quotiens forment une suite *symmétrique*, c'est-à-dire une suite $\alpha, \beta, \gamma \ldots \gamma, \beta, \alpha$, telle que les extrêmes soient égaux, ainsi que deux termes quelconques également éloignés des extrêmes, il est clair qu'on aura $\frac{q^{\circ}}{q} = \frac{p}{q}$, ou $q^{\circ} = p$. Réciproquement si on a $q^{\circ} = p$, on peut en conclure que la suite des quotiens est symmétrique.

On verra des exemples de ces suites dans le développement des racines quarrées des nombres en fraction continue.

## §. II. *Résolution des Équations indéterminées du premier degré.*

(12) Étant donnés deux nombres $a$ et $b$ premiers entr'eux, on pourra toujours résoudre en nombres entiers l'équation

$$ax - by = 1.$$

Pour cela, il faut réduire $\frac{a}{b}$ en fraction continue, et calculer la suite des fractions convergentes vers $\frac{a}{b}$. Soit $\frac{a^\circ}{b^\circ}$ celle qui précède $\frac{a}{b}$, on aura l'équation $ab^\circ - a^\circ b = \pm 1$. Si le signe + a lieu, on aura immédiatement $x = b^\circ$, $y = a^\circ$, ou plus généralement, en prenant une indéterminée $z$,

$$x = b^\circ + bz$$
$$y = a^\circ + az.$$

Si l'on a $ab^\circ - a^\circ b = -1$, alors on peut faire $x = -b^\circ$, $y = -a^\circ$, ou plus généralement

$$x = -b^\circ + bz$$
$$y = -a^\circ + az$$

$z$ étant une indéterminée qu'on peut prendre à volonté positive ou négative.

(13) En général, si on a à résoudre l'équation $ax - by = c$, $a$ et $b$ étant toujours premiers entr'eux, on cherchera de même, par les fractions continues, les nombres $a^\circ$ et $b^\circ$ qui donnent $ab^\circ - a^\circ b = \pm 1$, et de-là on conclura

$$x = bz \pm b^\circ c$$
$$y = az \pm a^\circ c.$$

Au moyen de l'indéterminée $z$, il est facile de trouver une solution telle que $x$ ne surpasse pas $\pm \frac{1}{2} b$, et une autre telle que $y$ ne surpasse pas $\pm \frac{1}{2} a$. En effet, si $b^\circ c$ surpasse $\frac{1}{2} b$, on peut prendre pour $z$ l'entier le plus proche de $\frac{b^\circ c}{b}$ et alors $b^\circ c - bz$ sera plus petit que $\frac{1}{2} b$.

On

On suppose que $a$ et $b$ n'ont point de commun diviseur ; car s'ils en avoient un, l'équation $ax - by = c$ ne pourroit avoir lieu, à moins que $c$ lui-même ne fût divisible par ce commun diviseur, et dans ce cas, il faudroit le faire disparoître par la division.

*Remarque.* Sans connoître les nombres $t$ et $u$ qui peuvent être indéterminés, il suffit de savoir que l'un de ces nombres $u$ est premier à un nombre donné $A$, et on pourra toujours supposer qu'il existe deux nombres $n$ et $z$, tels que $t = nu - Az$ ; on pourra supposer en même temps que $n$ n'excède pas $\frac{1}{2} A$. Cette propriété recevra par la suite un grand nombre d'applications.

(14) L'équation $ax - by = c$ que nous venons de résoudre satisfait à la question de trouver une valeur de $x$ telle que $\frac{ax - c}{b}$ soit un entier, condition que nous exprimerons ainsi $\frac{ax - c}{b} = e$. Or on peut avoir simultanément plusieurs conditions de cette sorte à remplir ; supposons qu'on demande une valeur de $x$ telle que les trois quantités

$$\frac{ax - c}{b}, \quad \frac{a'x - c'}{b'}, \quad \frac{a''x - c''}{b''}$$

soient des entiers. La première condition donnera une valeur de $x$ de la forme $x = m + bz$ : cette valeur étant substituée dans la seconde quantité, il faudra déterminer $z$ de manière que $\frac{a'bz + a'm - c'}{b'} = e$. Ici peut se manifester un signe d'impossibilité : car si $b$ et $b'$ ont un commun diviseur $\theta$, il est clair que l'équation précédente ne peut avoir lieu, à moins que le nombre déterminé $a'm - c'$ ne soit divisible aussi par $\theta$.

En général, la valeur de $z$ qui satisfait à la condition précédente (si elle n'est pas impossible) sera de la forme $z = n + b'z'$, ou $z = n + \frac{b'}{\theta} z'$, si $b'$ et $b$ ont un commun diviseur $\theta$. On aura donc $x = m + bn + bb'z'$, ou en général $x = m' + B'z'$, $B'$ étant le moindre nombre divisible à-la-fois par $b$ et $b'$. Cette valeur étant substituée dans la troisième quantité qui doit être un entier, on en

déduira la valeur finale de $x$, qui sera de la forme $x = M + Bz$, $B$ étant le moindre nombre divisible à-la-fois par $b, b', b''$, et $z$ étant une indéterminée. Ainsi on pourra toujours trouver une valeur de $x$ moindre ou non plus grande que $\frac{1}{2}B$ : et de cette première valeur on déduira toutes les autres, en lui ajoutant ou en en retranchant un multiple quelconque de $B$.

Lorsque les nombres sur lesquels on opère ne sont pas bien grands, il est aisé de satisfaire aux diverses conditions, sans avoir recours aux fractions continues. Cherchons, par exemple, un nombre $x$ tel que les trois quantités

$$\frac{3x-10}{7}, \quad \frac{11x+8}{17}, \quad \frac{16x-1}{5}$$

soient des entiers. La dernière quantité contient une partie entière $3x$, et un reste $\frac{x-1}{5}$; soit ce reste $= z$, on aura $x = 5z + 1$. Cette valeur, qui satisfait à la troisième condition, étant substituée dans la première, on aura $\frac{15z-7}{7} = e$, ou en supprimant l'entier, $\frac{z}{7} = e$; donc $z = 7u$, et $x = 35u + 1$. Il reste à substituer cette valeur dans la seconde quantité, et on aura $\frac{385u+19}{17} = e$. Supprimant l'entier contenu dans le premier membre, cette condition devient $\frac{11y+2}{17} = e$, ou $\frac{-6y+2}{17} = e$. Multipliant le premier membre par 3, et supprimant l'entier, on aura $\frac{-y+6}{17} = e$; donc $y = 6 + 17t$, et $x = 211 + 5.7.17t$; d'où l'on voit que le moindre nombre qni satisfait à la question est 211.

## §. III. *Méthode pour résoudre en nombres rationnels les Équations indéterminées du second degré.*

(15) Soit proposée l'équation générale

$$ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

dans laquelle $x$ et $y$ sont des indéterminées, et $a$, $b$, $c$, $d$, $e$, $f$ des nombres entiers donnés positifs ou négatifs; on tire d'abord de cette équation

$$2ax + by + d = \sqrt{[(by+d)^2 - 4a(cy^2 + ey + f)]}.$$

Ensuite si l'on fait, pour abréger, le radical $= t$, $b^2 - 4ac = A$, $bd - 2ae = g$, $d^2 - 4af = h$, on aura les deux équations

$$2ax + by + d = t$$
$$Ay^2 + 2gy + h = t^2.$$

Multiplions la dernière par $A$, et faisons de nouveau $Ay + g = u$, $g^2 - Ah = B$; nous aurons la transformée

$$u^2 - At^2 = B.$$

Réciproquement si on peut trouver des valeurs de $u$ et $t$ qui satisfassent à l'équation $u^2 - At^2 = B$, on en tirera les valeurs des indéterminées $x$ et $y$ de l'équation proposée, savoir :

$$y = \frac{u-g}{A}, \quad x = \frac{t - by - d}{2a}$$

où l'on doit observer que $u$ et $t$ peuvent être pris l'un et l'autre avec le signe qu'on voudra.

Si on cherche la solution de l'équation proposée en nombres rationnels, il suffira de résoudre par de tels nombres la transformée $u^2 - At^2 = B$; mais si on veut résoudre la proposée en nombres entiers, il faudra non-seulement que $t$ et $u$ soient des entiers, mais que les valeurs de $t$ et $u$ substituées dans celles de $x$ et $y$ donnent pour celles-ci des nombres entiers. Dans ce qui suit nous ne nous occuperons que de la résolution en nombres rationnels.

(16) Toute équation indéterminée du second degré peut se réduire, comme nous venons de le voir, à la forme $u^2 - At^2 = B$;

or quels que soient les nombres rationnels $t$ et $u$, on peut supposer qu'ils sont réduits à un même dénominateur. Ainsi, en faisant $u=\frac{x}{z}$, $t=\frac{y}{z}$, on aura à résoudre l'équation

$$x^2 - A y^2 = B z^2$$

dans laquelle maintenant $x$, $y$, $z$ sont des nombres entiers.

On peut supposer que ces trois nombres n'ont pas entr'eux un même commun diviseur ; car s'ils en avoient un, on le feroit disparoître par la division. De même on peut supposer que les nombres $A$ et $B$ n'ont aucun diviseur quarré ; car si on avoit, par exemple, $A = A'k^2$, $B = B'l^2$, on feroit $ky = y'$, $lz = z'$, et l'équation à résoudre deviendroit

$$x^2 - A'y'^2 = B'z'^2$$

dans laquelle $A'$ et $B'$ n'ont plus de facteur quarré.

L'équation $x^2 - Ay^2 = Bz^2$ étant ainsi préparée, on observera que deux quelconques des indéterminées $x$, $y$, $z$ ne peuvent avoir de commun diviseur ; car si $\theta^2$ divisoit $x^2$ et $y^2$, par exemple, il faudroit qu'il divisât $Bz^2$, or il ne peut diviser $z^2$, puisque les trois nombres $x$, $y$, $z$ n'ont point de commun diviseur ; il ne peut diviser non plus $B$, puisque $B$ n'a aucun facteur quarré. Donc $x$ et $y$ sont premiers entr'eux ; par la même raison $x$ et $z$ le sont, ainsi que $y$ et $z$.

Je dis de plus, que $A$ et $B$ peuvent être supposés positifs ; car on ne peut faire à l'égard des signes des termes de notre équation, que les trois suppositions suivantes :

$$x^2 - A y^2 = + B z^2$$
$$x^2 - A y^2 = - B z^2$$
$$x^2 + A y^2 = + B z^2$$

(J'omets la combinaison $x^2 + A y^2 = - B z^2$, parce qu'on voit bien qu'elle est impossible.)

De ces trois combinaisons, la seconde coincide avec la troisième par une simple transposition ; or si on multiplie celle-ci par $B$, et qu'on fasse $Bz = z'$, $AB = A'$, on aura

$$z'^2 - A'y^2 = Bx^2.$$

Donc l'équation à résoudre peut toujours être ramenée à la forme

$$x^2 - By^2 = A z^2,$$

dans laquelle $A$ et $B$ sont des nombres positifs et dégagés de tout facteur quarré.

(17) La méthode que nous allons suivre pour la résolution de cette équation, est celle qu'a donnée Lagrange dans les Mémoires de Berlin, année 1767 : elle consiste à opérer par des transformations la diminution successive des coefficiens $A$ et $B$, jusqu'à ce que l'un de ces coefficiens soit égal à l'unité, auquel cas la solution se déduit immédiatement des formules connues.

En effet, l'équation ainsi réduite est de la forme $x^2-y^2=Az^2$ ou $x^2-By^2=z^2$ ; mais ces deux formes n'en font qu'une, et ainsi il suffira d'indiquer la solution de la première $x^2-y^2=Az^2$. Pour cela, décomposons $A$ en deux facteurs $\alpha$, $\mathfrak{C}$ (lesquels seront toujours premiers entr'eux, puisque $A$ n'a pas de diviseur quarré), et imaginons que $z$ soit décomposé aussi en deux facteurs $p, q$, de sorte que l'on ait $A=\alpha\mathfrak{C}$, $z=pq$, on aura l'équation $(x+y)(x-y)=\alpha\mathfrak{C}p^2q^2$, à laquelle on satisfera généralement, en prenant $x+y=\alpha p^2$, $x-y=\mathfrak{C}q^2$, ce qui donnera

$$x=\frac{\alpha p^2+\mathfrak{C}q^2}{2},\; y=\frac{\alpha p^2-\mathfrak{C}q^2}{2},\; z=pq;$$

de sorte que les trois indéterminées $x, y, z$ seront exprimées au moyen de deux autres arbitraires $p$ et $q$; et s'il arrivoit que les valeurs de $x$ et de $y$ continssent la fraction $\frac{1}{2}$, on multiplieroit à-la-fois $x, y, z$ par 2.

Telle est la solution générale de l'équation $x^2-y^2=Az^2$, laquelle comprendra autant de formules particulières, qu'il y a de manières de décomposer $A$ en deux facteurs.

Par exemple, si $A=30$, il y a quatre manières de décomposer 30 en deux facteurs, savoir : 1.30, 2.15, 3.10, 5.6, et de-là résulteront ces quatre solutions de l'équation $x^2-y^2=30z^2$,

1°. $x=p^2+30q^2$, $y=p^2-30q^2$, $z=2pq$
2°. $x=2p^2+15q^2$, $y=2p^2-15q^2$, $z=2pq$
3°. $x=3p^2+10q^2$, $y=3p^2-10q^2$, $z=2pq$
4°. $x=5p^2+6q^2$, $y=5p^2-6q^2$, $z=2pq$.

(18) Venons à l'équation générale $x^2-By^2=Az^2$, et observons

d'abord que cette équation étant la même que $x^2 - Az^2 = y^2$, on peut, sans diminuer la généralité, supposer que le coefficient du second membre est le plus grand des deux. En cas d'égalité, la réduction que nous allons indiquer auroit toujours son effet.

Soit donc proposée l'équation $x^2 - By^2 = Az^2$ dans laquelle on suppose à-la-fois $A > B$, $A$ et $B$ positifs et dégagés de tout facteur quarré.

Nous avons déjà prouvé que $x$ et $y$ sont premiers entr'eux ; de-là il suit que $y$ et $A$ sont également premiers entr'eux, car si $y^2$ et $A$ avoient un commun diviseur $\theta$, il faudroit que $x^2$ fût aussi divisible par $\theta$, et ainsi $x^2$ et $y^2$ ne seroient pas premiers entr'eux.

Mais puisque $y$ et $A$ sont premiers entr'eux, si on suppose que l'équation proposée soit résoluble, et qu'ainsi on puisse trouver des valeurs déterminées de $x$ et $y$, telles que $x = M$, $y = N$, on pourra aussi ~~(n°. 13) satisfaire à~~ l'équation du premier degré

$$M = nN - y'A,$$

dans laquelle $M$, $N$, $A$ seroient des nombres donnés, premiers entr'eux, et $n$, $y'$ deux indéterminées.

Donc en général, sans connoître ces solutions particulières $x = M$, $y = N$, on peut supposer $x = ny - Ay'$, $n$ et $y'$ étant deux indéterminées, et en substituant cette valeur dans l'équation proposée, on aura, après avoir divisé par $A$,

$$\left(\frac{n^2 - B}{A}\right) y^2 - 2nyy' + Ay'^2 = z^2.$$

Mais puisque $y$ et $A$ sont premiers entr'eux, cette équation ne peut subsister, à moins que $\frac{n^2 - B}{A}$ ne soit égal à un entier. Soit cet entier $= A'k^2$, $k^2$ étant le plus grand quarré qui peut en être diviseur, on aura $n^2 - B = AA'k^2$, et l'équation à résoudre deviendra

$$A'k^2y^2 - 2nyy' + Ay'^2 = z^2.$$

Nous donnerons ci-après les moyens les plus simples pour déterminer un nombre $n$, de manière que $\frac{n^2 - B}{A}$ soit un entier. Il suffit, pour le présent, d'observer que s'il y a une valeur quelconque de $n$ qui rende $n^2 - B$ divisible par $A$, cette valeur peut être aug-

mentée ou diminuée d'un multiple quelconque de $A$, sans que $n^2 - B$ cesse d'être divisible par $A$; et ainsi on peut supposer que la valeur dont il s'agit est comprise entre les limites o et $A$, ou même entre les limites plus étroites $-\frac{1}{2}A$ et $+\frac{1}{2}A$.

De-là il suit, qu'en essayant successivement pour $n$ tous les nombres entiers depuis $-\frac{1}{2}A$ jusqu'à $+\frac{1}{2}A$, on en rencontrera nécessairement un ou plusieurs, qui rendront $n^2 - B$ divisible par $A$, si toutefois l'équation est résoluble; et dans le cas où aucun de ces nombres ne rendroit $n^2 - B$ divisible par $A$, on en conclura avec certitude que l'équation proposée n'est pas résoluble.

(19) Supposons donc qu'on a trouvé une ou plusieurs valeurs de $n$ qui aient la condition requise, il faudra, d'après chacune de ces valeurs, continuer le calcul de la manière suivante.

Reprenons l'équation $A'k^2y^2 - 2nyy' + Ay'^2 = z^2$, si on la multiplie par $A'k^2$, et qu'on fasse pour abréger,

$$A'k^2y - ny' = x', \quad kz = z',$$

la transformée sera

$$x'x' - By'y' = A'z'z'.$$

Cette transformée seroit résolue, si on connoissoit la solution de l'équation proposée, puisque les valeurs de $x'$, $y'$, $z'$ se concluent facilement de celles de $x$, $y$, $z$; réciproquement la proposée sera résolue, si on trouve la solution de sa transformée. Car des valeurs connues de $x'$, $y'$, $z'$ on peut également conclure celles de $x$, $y$, $z$: et il importe peu que celles-ci soient sous une forme entière ou fractionnaire, puisqu'il ne s'agit que de la résolution en nombres rationnels, et qu'après avoir trouvé des valeurs quelconques fractionnaires de $x$, $y$, $z$, on peut les réduire au même dénominateur, et supprimer le dénominateur commun.

Puisqu'on peut supposer le nombre $n < \frac{1}{2}A$, il est clair que $\frac{n^2 - B}{Ak^2}$ ou $A'$ sera $< \frac{1}{4}A$ et en même temps positif; car $n$ ne peut être $< \sqrt{B}$, puisqu'autrement $n^2 - B$ seroit $< B$, et ne pourroit être divisible par $A$. Donc l'équation proposée sera ramenée à une équation toute semblable, dans laquelle le coefficient $A'$ qui tient lieu de $A$ est moindre que $\frac{1}{4}A$.

(20) Si on a encore $A' > B$, on pourra semblablement de l'équation $x'^2 - By'^2 = A'z'^2$ déduire une seconde transformée

$$x''^2 - By''^2 = A''z''^2,$$

dans laquelle $A''$ sera $< \frac{1}{4}A'$ et toujours positif. Il n'y aura point de nouvelle condition à remplir pour obtenir cette seconde transformée, car ayant déjà trouvé

$$\frac{n^2 - B}{A'} = Ak^2,$$

si on fait $n = \mu A' + n'$, et qu'on prenne l'indéterminée $\mu$ de manière que $n'$ soit $< \frac{1}{2}A'$, il est facile de voir que $\frac{n'^2 - B}{A'}$ sera un entier positif moindre que $\frac{1}{4}A'$; on fera en conséquence

$$n'^2 - B = A'A''k'^2,$$

$A''$ étant plus petit que $\frac{1}{4}A'$ et ne renfermant aucun facteur quarré.

S'il arrive que $A''$ soit encore plus grand que $B$, on continuera ce système de transformées, où $B$ est constant, jusqu'à ce qu'on en trouve une

$$x^2 - By^2 = Cz^2$$

dans laquelle $C$ sera positif et $< B$.

(21) Mais après avoir fait passer dans le second membre le terme qui a le plus grand coefficient, ce qui donne

$$x^2 - Cz^2 = By^2,$$

on peut procéder semblablement à la réduction du coefficient $B$ par un second système de transformées

$$x'^2 - Cz'^2 = B'y'^2$$
$$x''^2 - Cz''^2 = B''y''^2$$
&c.

dans lesquelles les coefficiens $B'$, $B''$, &c. seront positifs, et diminueront suivant une raison au moins quadruple, et ainsi on parviendra bientôt à une transformée

$$x^2 - Cz^2 = Dy^2,$$

dans laquelle le coefficient $D$ sera moindre que $C$.

Or la suite des nombres positifs et décroissans $A$, $B$, $C$, $D$, &c. ne sauroit aller à l'infini; elle se terminera nécessairement par l'unité,

l'unité, et lorsqu'on sera arrivé à ce terme, la résolution de la dernière transformée, qui est donnée immédiatement, fera connoître celle de toutes les précédentes, et par conséquent celle de l'équation proposée.

Cette méthode n'est pas donnée ici comme la plus simple ni la plus courte, pour arriver à la résolution effective de l'équation proposée : mais la marche qu'elle prescrit pour opérer la diminution successive des coefficiens, est très-lumineuse, et nous en déduirons bientôt un théorême général sur la possibilité des équations indéterminées du second degré.

(22) Il est bon de prévenir une difficulté qui auroit lieu, si deux coefficiens étoient égaux.

Soit donc $A=B$ ; dans ce cas, pour faire en sorte que $\frac{n^2-B}{A}$ soit un entier, il semble qu'on doit faire $n=0$, et alors on auroit $A'k^2=-1$, ou $A'=-1$, ce qui ne s'accorde pas avec la supposition qu'on fait toujours que $A'$ est positif. Mais cette difficulté est facile à résoudre, car si au lieu de prendre $n=0$, on prend $n=A$, on aura $\frac{n^2-A}{A}=A-1$, ce qui seroit la valeur de $A'k^2$. On voit donc que l'équation $x^2-Ay^2=Az^2$ aura pour transformée $x'^2-Ay'^2=A'z'^2$ dans laquelle $A'$ sera $< A$ et positif. On feroit de même, si dans le cours de l'opération, on trouvoit $C=B$, ou $D=C$, &c.

Cette remarque fait voir, que dans le cas de $A=B$ et autres semblables, la méthode n'en est pas moins applicable, et qu'ainsi elle a toute la généralité nécessaire. Au reste, le cas dont il s'agit est susceptible d'être traité d'une manière plus simple et plus directe; car si on a l'équation $x^2-Ay^2=Az^2$, on voit d'abord que $x$ doit être divisible par $A$, et ainsi on peut faire $x=Au$, ce qui donnera

$$y^2+z^2=Au^2.$$

Dans cette équation, $z$ et $A$ sont premiers entr'eux (sans quoi $y$ et $z$ ne le seroient pas) ; ainsi on peut supposer $y=nz+Ay'$, ce qui donnera

$$\frac{n^2+1}{A}z^2+2nzy'+Ay'y'=u^2.$$

Celle-ci ne peut subsister, à moins que $\frac{n^2+1}{A}$ ne soit un entier, j'appelle cet entier $A'k^2$, $k^2$ étant le plus grand quarré qui en est diviseur, et j'aurai

$$A'k^2z^2 + 2nzy' + Ay'y' = u^2.$$

Multipliant de part et d'autre par $A'k^2$, et faisant $k^2A'z+ny'=z'$, $ku=u'$, on aura

$$z'z' + y'y' = A'u'u';$$

et ainsi l'équation proposée $z^2 + y^2 = Au^2$ sera ramenée à une équation de même forme dans laquelle $A'$ est positif et $< \frac{1}{4}A + \frac{1}{A}$. Continuant ainsi de transformée en transformée, les nombres positifs et décroissans $A$, $A'$, $A''$, &c. auront nécessairement pour terme l'unité, et alors la dernière équation étant résoluble immédiatement, on en déduira la solution de toutes les précédentes. Il n'y aura dans ce cas d'autre condition pour la possibilité de l'équation, que la première $\frac{n^2+1}{A}=e$, car les autres sont une suite de celle-là.

Dans la solution générale, au contraire, outre la première condition $\frac{n^2-B}{A}=e$, il faut qu'à mesure qu'on passe d'un systême de transformées à un autre systême, on puisse satisfaire aux diverses conditions $\frac{n'^2-C}{B}=e$, $\frac{n''^2-D}{C}=e$, et ainsi des autres. C'est ce qu'on examinera plus particulièrement dans le §. suivant.

## §. IV. *Théorème pour juger de la possibilité ou de l'impossibilité de toute équation indéterminée du second degré.*

(23) On a fait voir dans le paragraphe précédent, que toute équation indéterminée du second degré peut se réduire à la forme

$$x^2 - By^2 = Az^2$$

dans laquelle $A$ et $B$ sont des nombres entiers positifs, dégagés de tout facteur quarré, et où l'on a en même tems $A > B$.

Cela posé, pour procéder à la résolution, il faut d'abord déterminer un nombre $\alpha$ non plus grand que $\frac{1}{2}A$, tel que $\frac{\alpha^2 - B}{A}$ soit un entier. Ce nombre étant trouvé, on forme la suite d'équations:

$$\begin{array}{ll} \alpha^2 - B = A\ A'\ k^2 & \alpha' = \mu\ A' \pm \alpha \quad < \frac{1}{2} A' \\ \alpha'^2 - B = A'\ A''\ k'^2 & \alpha'' = \mu'\ A'' \pm \alpha' \quad < \frac{1}{2} A'' \\ \alpha''^2 - B = A''\ A'''\ k''^2 & \&c. \\ \&c. & \end{array}$$

Dans la première $A'k^2$ est le quotient de $\alpha^2 - B$ divisé par $A$, $k^2$ est le plus grand quarré qui divise $A'k^2$, en sorte que $A'$ ne renferme plus que des facteurs simples, ainsi que $A$ et $B$, et c'est ce qu'on observera dans les autres valeurs semblables. $A'$ étant déterminé, on a $\alpha'$ par l'équation $\alpha' = \mu A' \pm \alpha$, ayant soin de prendre l'indéterminée $\mu$, de manière que $\alpha'$ soit $< \frac{1}{2} A'$, (le signe $<$ n'excluant pas l'égalité). $\alpha'$ étant connu, $\alpha'^2 - B$ est nécessairement divisible par $A'$; on désigne le quotient par $A''k'^2$, et on continue de même à former les autres équations.

Au moyen de ces opérations, la suite $A$, $A'$, $A''$, &c. dont chaque terme est positif et moindre que le quart du précédent, décroîtra d'une manière rapide, jusqu'à ce qu'on parvienne à un terme $A^{(n)}$ ou $C$ moindre que $B$; et l'équation proposée aura pour

transformées successives les équations suivantes (où pour plus de simplicité je laisse les indéterminées sans accens):

$$x^2 - By^2 = A' z^2$$
$$x^2 - By^2 = A'' z^2$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$x^2 - By^2 = Cz^2.$$

équations tellement liées entr'elles, que si on connoît la solution d'une seule, on aura immédiatement celle de toutes les autres, et par conséquent celle de l'équation proposée.

Dans ce premier système de transformées, il n'y a aucune condition à remplir, si ce n'est la première $\frac{n^2 - B}{A} = e$.

Mais puisque $C$ est $< B$, la dernière transformée étant mise sous la forme

$$x^2 - Cz^2 = By^2,$$

il faudra, pour qu'elle soit résoluble, qu'on puisse trouver un nombre $\theta$ tel que $\theta^2 - C$ soit divisible par $B$; cette condition étant remplie, on procédera à la diminution de $B$ par un second système de transformées,

$$x^2 - Cz^2 = B' y^2$$
$$x^2 - Cz^2 = B'' y^2$$
$$\cdot$$
$$\cdot$$
$$x^2 - Cz^2 = D y^2$$

dans lequel la suite $B, B', B''\ldots$ sera prolongée jusqu'à ce qu'on parvienne à un terme $D < C$.

On continuera ainsi la suite des nombres entiers décroissans $A, B, C, D$, &c. jusqu'à ce qu'on parvienne à un terme égal à l'unité, et alors la question sera résolue.

(24) Il est aisé de voir qu'on ne sera arrêté nulle part dans le cours de cette opération, lorsqu'à l'égard d'une transformée quelconque,

$$x^2 - Fy^2 = G z^2$$

on pourra satisfaire aux deux conditions $\frac{\lambda^2 - F}{G} = e$, $\frac{\mu^2 - G}{F} = e$.

Or il suffit que ces deux conditions soient remplies dans l'équation proposée $x^2 - By^2 = A z^2$, et dans sa première transformée $x^2 - By^2 = A' z^2$, et nous allons prouver qu'elles le seront dans toutes les autres; de sorte qu'alors l'équation proposée sera nécessairement résoluble.

Supposant donc que les deux conditions mentionnées ont lieu dans les deux premières équations

$$x^2 - B y^2 = A z^2$$
$$x^2 - B y^2 = A' z^2 :$$

c'est-à-dire qu'il y a des entiers $\alpha$, $\mathcal{C}$, $\alpha'$, $\mathcal{C}'$ tels que

$$\frac{\alpha^2 - B}{A}, \quad \frac{\alpha'^2 - B}{A'}, \quad \frac{\mathcal{C}^2 - A}{B}, \quad \frac{\mathcal{C}'^2 - A'}{B}$$

sont des entiers, il faut prouver que les conditions semblables ont lieu dans la transformée suivante

$$x^2 - B y^2 = A'' z^2.$$

Or comme on a déjà $\dfrac{\alpha'' \alpha'' - B}{A''} = A' k'^2$, il suffit de faire voir qu'il existe un entier $\mathcal{C}''$ tel que $\dfrac{\mathcal{C}'' \mathcal{C}'' - A''}{B} = e$.

Soit $\theta$ l'un des nombres premiers qui divisent $B$, on a déjà, par les conditions données :

$$\frac{\mathcal{C}^2 - A}{\theta} = e, \quad \frac{\mathcal{C}'^2 - A'}{\theta} = e.$$

Cherchons d'après cela un nombre $\lambda$ tel que $\dfrac{\lambda^2 - A''}{\theta} = e$. Si $A''$ est divisible par $\theta$, il n'y a aucune difficulté; soit donc $A''$ non divisible par $\theta$, je distingue deux cas, selon que $\theta$ divise ou ne divise pas $A'$.

1°. Si $\theta$ divise $A'$, il divisera $\alpha$ et $\alpha'$ en vertu des équations

$$\alpha^2 - B = A A' k^2, \quad \alpha' = \mu A' \pm \alpha.$$

D'ailleurs on a

$$A'' k' k' = \frac{\alpha' \alpha' - B}{A'} = \frac{(\mu A' \pm \alpha)^2 - B}{A'} = \mu^2 A' \pm 2 \mu \alpha + A k^2,$$

donc $\dfrac{A k^2 - A'' k' k'}{\theta}$ est un entier; ajoutant $\dfrac{\mathcal{C}^2 k^2 - A k^2}{\theta}$ qui en est

un, on aura $\frac{\zeta^2 k^2 - A'' k' k'}{\theta} = e$. Mais $k'$ est premier à $B$, et par conséquent à $\theta$, puisque si $k'$ et $B$ avoient un commun diviseur, il faudroit, d'après l'équation $\alpha'^2 - B = A' A'' k'^2$, que $B$ eût un facteur quarré, ce qui est contre la supposition; donc on peut faire $k\zeta = nk' - m\theta$, et ainsi on aura $\frac{n^2 k' k' - A'' k' k'}{\theta} = e$, ou simplement $\frac{n^2 - A''}{\theta} = e$.

2°. Si $\theta$ ne divise pas $A'$, ni par conséquent $\zeta'$, de l'équation $\frac{\zeta' \zeta' - A'}{\theta} = e$ on déduira d'abord $\frac{A'' k' k' \zeta' \zeta' - A' A'' k' k'}{\theta} = e$, ou $\frac{A'' k'^2 \zeta'^2 - \alpha'^2}{\theta} = e$. Ensuite, puisqne $\zeta' k'$ et $\theta$ sont premiers entr'eux, on pourra faire $\alpha' = n \zeta' k' - m\theta$, ce qui donnera $\frac{n^2 - A''}{\theta} = e$.

D'après cette démonstration, qui a lieu pour tous les facteurs premiers de $B$, on voit que non-seulement l'éqnation $\frac{\zeta'' \zeta'' - A''}{B} = e$ est possible, mais qu'il est facile de trouver *a priori* la valeur de $\zeta''$. Donc toutes les équations $x^2 - By^2 = A'' z^2$, $x^2 - By^2 = A''' z^2$, &c. où $B$ est le même, n'offriront aucun signe d'impossibilité.

Nous allons faire voir maintenant que la même chose a lieu dans le second systême de transformées où, en conservant une même valeur de $C$, on fait parcourir à $B$ la suite décroissante $B'$, $B''$, &c.

(25) Les deux dernières équations du premier systême étant

$$x^2 - By^2 = A^{(n-1)} z^2$$
$$x^2 - By^2 = A^{(n)} z^2 = Cz^2$$

(où $n$ et $n-1$ sont des indices et non des exposans), on peut supposer que ces équations satisfont déjà aux conditions

$$\frac{\alpha^2 - B}{A^{n-1}} = e, \quad \frac{\zeta^2 - A^{n-1}}{B} = e, \quad \frac{\alpha'^2 - B}{A^n} = e, \quad \frac{\zeta'^2 - A^n}{B} = B' f^2;$$

et il s'agit de prouver qne dans la transformée suivante,

$x^2 - A^n y^2 = B' z^2$ (qui appartient au second système), on peut satisfaire aux deux conditions

$$\frac{\varphi^2 - A^n}{B} = e\,, \quad \frac{\psi^2 - B'}{A^n} = e.$$

Or la première est immédiatement remplie par l'équation $\frac{\zeta'^2 - A^n}{B'} = Bf^2$, il reste donc à faire voir qu'on peut toujours satisfaire à la seconde $\frac{\psi^2 - B'}{A^n} = e$.

Désignons par $\theta$ l'un des nombres premiers qui divisent $A^n$, et cherchons le nombre $\psi$ tel que $\frac{\psi^2 - B'}{\theta} = e$. Si $B'$ est divisible par $\theta$, on aura $\psi = 0$, ou un multiple de $\theta$. Si $B'$ n'est pas divisible par $\theta$, il y aura deux cas à considérer.

1°. Si $\theta$ est diviseur de $B$, il le sera de $\alpha$ et de $\zeta'$, en vertu des équations $\alpha^2 - B = A^n A^{n-1} k^2$, $\zeta'\zeta - A^n = BB'f^2$; on pourra donc établir cette suite d'entiers qui dérivent les uns des autres par des substitutions ou opérations très-simples :

$$\frac{\zeta^2 - A^{n-1}}{\theta} = e\,, \quad \frac{k^2\zeta^2 A^n - k^2 A^n A^{n-1}}{\theta\theta} = e\,, \quad \frac{k^2\zeta^2 A^n + B}{\theta\theta} = e\,,$$

$$\frac{(\zeta'\zeta - BB'f^2)k^2\zeta^2 + B}{\theta\theta} = e, \quad \frac{BB'f^2k^2\zeta^2 - B}{\theta\theta} = e, \quad \frac{B'f^2k^2\zeta^2 - 1}{\theta} = e,$$

$$\frac{B'B'f^2k^2\zeta^2 - B'}{\theta} = e.$$

Soit donc $\psi = B'fk\zeta$, et on aura $\frac{\psi^2 - B'}{\theta} = e$.

2°. Si $\theta$ ne divise pas $B$, il ne divisera ni $\alpha$, ni $\zeta'$, on aura donc successivement

$$\frac{\alpha^2 - B}{\theta} = e\,, \quad \frac{\alpha^2 f^2 B' - f^2 BB'}{\theta} = e\,, \quad \frac{\alpha^2 f^2 B' - \zeta'\zeta'}{\theta} = e.$$

Mais $\alpha f$ et $\theta$ étant premiers entr'eux, on peut supposer $\zeta' = \psi\alpha f - m\theta$, ce qui donnera $\frac{\psi^2 - B'}{\theta} = e$.

Le même raisonnement ayant lieu par rapport à tous les diviseurs

premiers de $A'$, il s'ensuit qu'on pourra toujours satisfaire à l'équation $\frac{\psi^2 - B'}{A'} = e$.

(26) Donc l'équation $x^2 - By^2 = Az^2$ sera résoluble, si l'on peut satisfaire aux deux conditions $\frac{\alpha^2 - B}{A} = e$, $\frac{\beta^2 - A}{B} = e$, et si, de plus, dans la première transformée $x^2 - By^2 = A'z^2$, on peut satisfaire à la troisième condition $\frac{\beta\beta' - A'}{B} = e$.

Cette dernière condition seroit superflue, comme on va bientôt le démontrer, si les deux nombres $A$ et $B$ étoient premiers entre eux; mais la proposition générale est susceptible d'être présentée d'une manière à-la-fois plus simple et plus élégante.

Observons d'abord que toute équation indéterminée du second degré peut être ramenée à la forme $ax^2 + by^2 = cz^2$ dans laquelle les coefficiens $a$, $b$, $c$ sont positifs, n'ont deux à deux aucun diviseur commun, et de plus sont dégagés de tout facteur quarré. Ce qui regarde les signes est manifeste, puisque toute équation formée avec trois quantités, exige qu'une de ces quantités soit égale à la somme des deux autres. Ensuite si $a$ contenoit un facteur quarré $\theta^2$, on feroit $a = \theta^2 a'$, $x = \theta x'$, et le terme $ax^2$ se changeroit en $a'x'^2$, où $a'$ n'a plus de facteur quarré. Enfin, si deux des trois coefficiens $a$, $b$, $c$, par exemple, $a$ et $b$, avoient un diviseur commun $\theta$, on feroit $a = a'\theta$, $b = b'\theta$, $c\theta = c'$, $z = z'\theta$, et l'équation $ax^2 + by^2 = cz^2$, seroit changée en une autre $a'x^2 + b'y^2 = c'z'^2$ dans laquelle $a'$ et $b'$ n'ont plus de commun diviseur.

Cela posé, la nouvelle équation $ax^2 + by^2 = cz^2$ étant mise sous la forme $\left(\frac{cz}{x}\right)^2 - bc\left(\frac{y}{x}\right)^2 = ac$, peut être assimilée à la formule $x^2 - By^2 = Az^2$, et la comparaison donnera $B = bc$, $A = ac$. On aura donc d'abord les deux conditions à remplir

$$\frac{\alpha^2 - bc}{ac} = e, \quad \frac{\beta^2 - ac}{bc} = e.$$

Soit

Soit $\alpha = c\mu$, $\beta = c\nu$, ces conditions deviendront

$$\frac{c\mu^2 - b}{a} = e, \quad \frac{c\nu^2 - a}{b} = e.$$

Pour exprimer la troisième $\frac{\beta'\beta' - \mathcal{A}'}{B} = e$, observons qu'on a $\alpha^2 - B = \mathcal{A}\mathcal{A}'k^2$, ou $c\mu^2 - b = a\mathcal{A}'k^2$, et comme $ak^2$ n'a point de diviseur commun avec $bc$, la dernière condition sera remplie si l'on a

$$\frac{ak^2\beta'\beta' - c\mu^2 + b}{bc} = e.$$

Or pour que le numérateur de cette quantité soit divisible par $b$, il suffit que $ak^2\beta'\beta' - c\mu^2$ le soit, ou bien mettant $c\nu^2$ au lieu de $a$ en vertu de la seconde condition, il faudra que $k^2\beta'^2\nu^2 - \mu^2$ soit divisible par $b$, ce qui est toujours possible, en déterminant $\beta'$ d'après l'équation $\frac{k\nu\beta' \pm \mu}{b} = e$. De-là on voit que lorsque $\mathcal{A}$ et $B$ n'ont pas de commun diviseur (ou lorsque $c = 1$), la troisième condition est remplie par une suite des deux autres.

Mais s'ils ont un commun diviseur $c$, il restera encore à satisfaire à la condition $\frac{ak^2\beta'\beta' + b}{c} = e$, ou simplement $\frac{a\lambda^2 + b}{c} = e$.

Voici donc un théorême général, d'après lequel on pourra décider immédiatement, et sans aucune transformation, si une équation indéterminée du second degré est résoluble ou ne l'est pas.

### Théorême.

(27) Etant proposée l'équation $ax^2 + by^2 = cz^2$ dans laquelle les coefficiens $a$, $b$, $c$, pris individuellement, ou deux à deux, n'ont ni diviseur quarré, ni diviseur commun, je dis que cette équation sera résoluble, si on peut trouver trois entiers $\lambda$, $\mu$, $\nu$ tels que les trois quantités

$$\frac{a\lambda^2 + b}{c}, \quad \frac{c\mu^2 - b}{a}, \quad \frac{c\nu^2 - a}{b}$$

soient des entiers : elle sera au contraire insoluble, si ces trois conditions ne peuvent être remplies à-la-fois.

*Remarque I.* Ces conditions se réduisent à deux, si l'un des trois nombres $a$, $b$, $c$ est égal à l'unité, et elles se réduisent à une seule, comme dans le n°. 22, si deux de ces nombres sont égaux à l'unité.

*Remarque II.* On peut toujours arranger les trois termes de l'équation proposée, de manière que $a$, $b$, $c$ soient positifs; mais cette condition n'est pas de rigueur, et le théorême seroit encore vrai, quand même quelqu'un de ces termes seroit négatif.

Il ne faudroit pas cependant conclure de-là qu'une équation telle que $x^2+5y^2+6z^2=0$ est possible, par cela seul qu'on peut satisfaire aux conditions $\frac{\lambda^2+5}{6}=e$, $\frac{\mu^2+6}{5}=e$, il faudroit conclure seulement qu'elle peut se ramener à la forme $x^2+y^2+z^2=0$. En général, toute équation résoluble pourra, par la méthode du §. précédent, se ramener à la forme $x^2+y^2-z^2=0$, mais il suffit de la ramener à la forme $Ax^2+y^2-z^2=0$, dont la solution se trouve immédiatement.

---

## §. V. *Développement de la racine d'un nombre non quarré en fraction continue.*

(28) Le principe exposé n°. 1, pour développer une quantité quelconque $x$ en fraction continue, s'applique avec beaucoup de facilité aux racines quarrées des nombres, et en général aux quantités de la forme $\frac{\sqrt{A}+B}{C}$, $A$, $B$ et $C$ étant des nombres entiers. Mais pour qu'on voie plus clairement la marche de l'opération, nous prendrons d'abord un exemple particulier.

Soit $A=19$, on aura $x$ ou $\sqrt{19}=4+\frac{1}{x'}$; de-là $x'=\frac{1}{\sqrt{19}-4}$: ou, en multipliant les deux termes de la fraction par $\sqrt{19}+4$,

$x' = \frac{\sqrt{19}+4}{3}$ : l'entier le plus grand compris dans cette quantité est 2, ainsi on aura $x' = 2 + \frac{\sqrt{19}-2}{3}$. Cette dernière partie étant nommée $\frac{1}{x''}$, on en tire $x'' = \frac{3}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{5}$ ; l'entier compris est 1 et le reste $\frac{\sqrt{19}-3}{5}$ qu'il faut renverser de même pour avoir la valeur de $x'''$, ainsi de suite. Voici donc l'opération pour développer $\sqrt{19}$ en fraction continue :

$$x = \sqrt{19} \qquad = 4 + \frac{\sqrt{19}-4}{1}$$

$$x' = \frac{1}{\sqrt{19}-4} = \frac{\sqrt{19}+4}{3} = 2 + \frac{\sqrt{19}-2}{3}$$

$$x'' = \frac{3}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{5} = 1 + \frac{\sqrt{19}-3}{5}$$

$$x''' = \frac{5}{\sqrt{19}-3} = \frac{\sqrt{19}+3}{2} = 3 + \frac{\sqrt{19}-3}{2}$$

$$x^{\text{iv}} = \frac{2}{\sqrt{19}-3} = \frac{\sqrt{19}+3}{5} = 1 + \frac{\sqrt{19}-2}{5}$$

$$x^{\text{v}} = \frac{5}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{3} = 2 + \frac{\sqrt{19}-4}{3}$$

$$x^{\text{vi}} = \frac{3}{\sqrt{19}-4} = \frac{\sqrt{19}+4}{1} = 8 + \frac{\sqrt{19}-4}{1}$$

$$x^{\text{vii}} = \frac{1}{\sqrt{19}-4} = \frac{\sqrt{19}+4}{3} = 2 \quad \text{\&c.}$$

Arrivés à ce terme, on tombe sur une valeur de $x^{\text{vii}}$ égale à celle de $x'$, d'où il suit que les quotiens déjà trouvés 2, 1, 3, 1, 2, 8 reviendront dans le même ordre, et qu'ainsi le développement de $\sqrt{19}$ en fraction continue donnera les quotiens

4 : 2, 1, 3, 1, 2, 8 : 2, 1, 3, 1, 2, 8 : 2, 1, 3, 1, 2, 8 : &c.
où l'on voit que la période 2, 1, 3, 1, 2, 8 revient toujours dans le même ordre, et se répète à l'infini.

(29) Soit maintenant $A$ un nombre quelconque, $a^2$ le plus grand quarré compris, et $b$ le reste, en sorte qu'on ait $A = a^2 + b$,

le développement de $\sqrt{A}$ en fraction continue donnera d'abord

$$x = \sqrt{A} = a + \frac{\sqrt{A} - a}{1}$$

$$x' = \frac{1}{\sqrt{A} - a} = \frac{\sqrt{A} + a}{b} = \text{\&c.}$$

Supposons qu'en prolongeant indéfiniment l'opération, on parvienne au quotient-complet $x^{(n)}$ ou $y = \frac{\sqrt{A} + I}{D}$; soit $\mu$ l'entier compris dans $y$, le reste sera $\frac{\sqrt{A} + I - \mu D}{D}$; ce reste étant nommé $\frac{1}{y'}$ on aura $y' = \frac{D}{\sqrt{A} + I - \mu D}$, et puisque d'ailleurs l'analogie des formes exige qu'on ait $y' = \frac{\sqrt{A} + I'}{D'}$, on tirera de-là l'équation suivante pour déterminer $I'$ et $D'$:

$$\frac{D}{\sqrt{A} + I - \mu D} = \frac{\sqrt{A} + I'}{D'}.$$

Cette équation, où il faut égaler séparément la partie rationnelle à la partie rationnelle et la partie irrationnelle à la partie irrationnelle, donnera

$$I' = \mu D - I$$
$$D' = \frac{A - I'I'}{D}.$$

Telle est la loi très-simple par laquelle d'un quotient-complet quelconque $\frac{\sqrt{A} + I}{D}$, on déduira le quotient-complet suivant $\frac{\sqrt{A} + I'}{D'}$; et il n'est pas à craindre que les nombres $I'$ et $D'$ soient fractionnaires, car si on substitue la valeur de $I'$ dans celle de $D'$, on aura $D' = \frac{A - (\mu D - I)^2}{D} = \frac{A - I^2}{D} + 2\mu I - \mu^2 D$. Or ayant $A - I^2 = D' D$, si on désigne par $\frac{\sqrt{A} + I^0}{D^0}$ le quotient-complet qui précède $\frac{\sqrt{A} + I}{D}$, on aura semblablement $A - I^2 = D D^0$, donc

$$D' = D^0 + 2\mu I - \mu^2 D.$$

D'où l'on voit que puisque les nombres $D$ et $I$ sont entiers dans les deux premiers quotiens-complets $\frac{\sqrt{A}+0}{1}$, $\frac{\sqrt{A}+a}{b}$, ils le seront nécessairement dans tous les autres à l'infini.

La valeur qu'on vient de trouver pour $D'$, peut aussi se mettre sous la forme $D'=D^\circ+\mu\,(I-I')$; ainsi des deux quotiens-complets consécutifs

$$\frac{\sqrt{A}+I^\circ}{D^\circ}=\mu^\circ+$$
$$\frac{\sqrt{A}+I}{D}=\mu\ +$$

on déduira le quotient-complet suivant $\frac{\sqrt{A}+I'}{D'}$, au moyen des formules $I'=\mu D-I$, $D'=D^\circ+\mu\,(I-I')$; ce qui réduit la loi de continuation à un grand degré de simplicité.

(30) Supposons maintenant que $\frac{p^\circ}{q^\circ}$, $\frac{p}{q}$ soient deux fractions consécutives convergentes vers $\sqrt{A}$; soit $\frac{\sqrt{A}+I}{D}$ le quotient complet qui répond à la fraction $\frac{p}{q}$, on aura, suivant le principe connu,

$$\sqrt{A}=\frac{p\left(\frac{\sqrt{A}+I}{D}\right)+p^\circ}{q\left(\frac{\sqrt{A}+I}{D}\right)+q^\circ}=\frac{p\sqrt{A}+pI+p^\circ D}{q\sqrt{A}+qI+q^\circ D}$$

d'où l'on tire les deux équations

$$pI+p^\circ D=qA$$
$$qI+q^\circ D=p$$

lesquelles donnent

$$(pq^\circ-p^\circ q)\,I=qq^\circ A-pp^\circ$$
$$(pq^\circ-p^\circ q)\,D=pp-Aqq.$$

Or, par la propriété des fractions continues (n°. 6) on a $pq^\circ-p^\circ q=+1$, si $\frac{p}{q}$ est $>\sqrt{A}$, et $pq^\circ-p^\circ q=-1$, si $\frac{p}{q}$ est $<\sqrt{A}$, d'où l'on

voit que $pq^{\circ} - p^{\circ}q$ a toujours le même signe que $pp - Aqq$, et qu'ainsi $D$ est toujours positif. Ces valeurs prouvent encore immédiatement que $D$ et $I$ sont toujours des entiers; je dis de plus que $I$ est toujours positif; car d'un côté l'équation $qI + q^{\circ}D = p$ donne $\frac{q^{\circ}}{q} = \left(\frac{p}{q} - I\right) : D$, et puisque $q^{\circ}$ est $< q$, il faut qu'on ait $D > \frac{p}{q} - I$, ou $D > \sqrt{A} - I$; d'un autre côté, on a $\frac{\sqrt{A} + I}{D} > \mu$, donc $D < \sqrt{A} + I$. Or ces deux conditions seroient incompatibles, si $I$ étoit négatif.

Cela posé, il est facile de trouver les limites que les nombres $I$ et $D$ ne peuvent surpasser; l'équation $A - I^2 = DD^{\circ}$ donne $I < \sqrt{A}$, ainsi $I$ ne sauroit excéder l'entier $a$ compris dans $\sqrt{A}$, et puisqu'on a d'ailleurs $I' + I = \mu D$, il s'ensuit que $2a$ est la limite de $D$, et en même temps celle du quotient $\mu$.

Mais puisque la fraction continue qui représente la valeur d'une quantité irrationnelle doit s'étendre à l'infini, et qu'il ne peut y avoir qu'un certain nombre de valeurs différentes tant pour $I$ que pour $D$, il est nécessaire que la même valeur de $I$ se rencontre une infinité de fois avec la même valeur de $D$; or dès que l'on retrouve pour le quotient-complet $\frac{\sqrt{A} + I}{D}$ une valeur déjà trouvée, il est clair que les quotiens ou termes de la fraction continue doivent être les mêmes et dans le même ordre que ceux qu'on a déjà obtenus; donc la fraction continue qui exprime $\sqrt{A}$ sera composée (au moins après quelques termes) d'une période constante qui se répétera à l'infini, comme on l'a déjà vu dans un cas particulier, n°. 28.

(31) Il s'agit présentement de déterminer le point précis où commence la période. Nous supposerons que cette période est $\mu, \mu', \mu'' \ldots \omega$, et nous désignerons à l'ordinaire la suite des quotiens, et celle des fractions convergentes qui leur répondent jusqu'au commencement de la seconde période, comme il suit:

Quotiens $a$, $\alpha$, $\beta$, $\gamma$ .......... $\lambda$, $\mu$, $\mu'$, $\mu''$ .......... $\omega$, $\mu$, $\mu'$, $\mu''$.. $\omega$, &c.

Fract. converg. $\left\{ \frac{1}{0}, \frac{a}{1} \right.$ .................. $\frac{p^\circ}{q^\circ}$, $\frac{p}{q}$ .................. $\frac{p^\circ 1}{q^\circ 1}$, $\frac{p 1}{q 1}$ ..................

Soient en même tems les valeurs correspondantes du quotient-complet

$$\frac{\sqrt{A}}{1},\ \frac{\sqrt{A}+a}{b} \ldots\ldots \frac{\sqrt{A}+I^\circ}{D^\circ},\ \frac{\sqrt{A}+I}{D} \ldots\ldots \frac{\sqrt{A}+I^\circ 1}{D^\circ 1},\ \frac{\sqrt{A}+I}{D} \ldots\ldots$$

on aura d'abord, par ce qui a été démontré, $A - I^{\circ 2} = DD^\circ$, et $A - I^{\circ 2} = DD^\circ 1$, ce qui donne $D^\circ 1 = D^\circ$, on aura aussi $I = \lambda D^\circ - I^\circ$ et $I = \omega D^\circ 1 - I^\circ 1$, d'où l'on tire $\frac{I^\circ - I^\circ 1}{D^\circ} = \lambda - \omega$. Mais d'un autre côté, l'équation $q\,I + q^\circ D = p$, donne $I = \frac{p}{q} - \frac{q^\circ D}{q}$; et puisque $\frac{p}{q}$ est une valeur approchée de $\sqrt{A}$, on doit avoir $\frac{p}{q} = a +$ une fraction $\frac{r}{q}$, d'où résulte

$$a - I = \frac{q^\circ D - r}{q};$$

donc à cause de $q^\circ < q$, on aura $a - I < D$; on aura semblablement $a - I^\circ < D^\circ$, $a - I^\circ 1 < D^\circ 1$; donc à plus forte raison $I^\circ - I^\circ 1 < D^\circ$. Mais on a trouvé $\frac{I^\circ - I^\circ 1}{D^\circ} =$ à l'entier $\lambda - \omega$, donc il faut que cet entier soit zéro; donc on aura $I^\circ = I^\circ 1$ et $\lambda = \omega$.

On démontrera de même que le quotient qui précède $\lambda$ est égal à celui qui précède $\omega$, et ainsi de suite jusqu'au quotient $\alpha$; de sorte que le quotient $\alpha$ est celui qui revient le premier, et qui doit commencer la période.

(32) Cela posé, on peut représenter ainsi la série des quotiens et celle des fractions convergentes qui leur répondent dans le développement de $\sqrt{A}$.

Qnotiens ..... $a$; $\alpha$, $\beta$ .... $\lambda$, $\mu$; $\alpha$, $\beta$, $\gamma$ .. $\lambda$, $\mu$; $\alpha$, $\beta$, ... $\lambda$, $\mu$; &c.

Fract. converg. $\frac{1}{0}$, $\frac{a}{1}$, ..... $\frac{p^\circ}{q^\circ}$, $\frac{p}{q}$, $\frac{p'}{q'}$, .... $\frac{p^\circ 1}{q^\circ 1}$, $\frac{p 1}{q 1}$, $\frac{p' 1}{q' 1}$, ..............

Dans cette disposition, $\frac{p}{q}$ est la fraction convergente qui répond au dernier quotient $\mu$ de la première période $\alpha, \beta \ldots \lambda, \mu$; soit $z$ le quotient-complet correspondant, on aura $z-\mu=\sqrt{A}-a$, ou $z=\mu-a+\sqrt{A}$, et il en résultera, suivant le principe ordinaire,

$$\sqrt{A}=\frac{pz+p^\circ}{qz+q^\circ}=\frac{p\sqrt{A}+p(\mu-a)+p^\circ}{q\sqrt{A}+q(\mu-a)+q^\circ};$$

ce qui fournit les deux équations

$$p(\mu-a)+p^\circ=Aq$$
$$q(\mu-a)+q^\circ=p.$$

La seconde équation donne $\mu-a+\frac{q^\circ}{q}=\frac{p}{q}$, d'où il suit que $\mu-a$ est le plus grand entier compris dans $\frac{p}{q}$; cet entier est égal à $a$, ainsi on a $\mu-a=a$, ou $\mu=2a$. En même temps, puisque $q^\circ=p-aq$, il s'ensuit que la série des quotiens $\alpha, \beta, \ldots \theta, \lambda$ qui précèdent $\mu$ est symmétrique (n°. 11), car $\frac{p-aq}{q}$ est l'une des fractions convergentes vers $\sqrt{A}-a$, quantité égale à la fraction continue $\frac{1}{\alpha+}\frac{1}{\beta+\&c.}$, et cette fraction convergente est précédée de $\frac{p^\circ-aq^\circ}{q^\circ}$; donc puisqu'on a $q^\circ=p-aq$, il faut que la période $\alpha, \beta, \ldots \theta, \lambda$ soit identique avec son inverse $\lambda, \theta \ldots \beta, \alpha$. Et de toutes ces remarques, il suit que les quotiens provenans du développement de $\sqrt{A}$ procèdent suivant cette loi :

$$a; \alpha, \beta, \gamma \ldots \gamma, \beta, \alpha, 2a; \alpha, \beta, \gamma \ldots \gamma, \beta, \alpha, 2a; \&c.$$

loi qui deviendroit encore plus régulière, si le premier quotient étoit $2a$ ou zéro; c'est-à-dire s'il s'agissoit du développement de $\sqrt{A}\pm a$.

Il est important d'observer, que toute fraction convergente $\frac{p}{q}$, qui répond au quotient $2a$ dans une période quelconque, est telle qu'on a $p^2-Aq^2=\pm 1$. Car lorsque le quotient $\mu=2a$, l'équation $I^\circ+I=D\mu$, où $I$ et $I^\circ$ ne peuvent excéder $a$ (n°. 30), donnera nécessairement $I=I^\circ=a$, et $D=1$, donc l'équation $(pq^\circ-p^\circ q)$

$(pq' - p'q)\,D = p^2 - A\,q^2$, devient $p^2 - A\,q^2 = \pm 1$, savoir $+1$, si $\frac{p}{q}$ est $> \sqrt{A}$, et $-1$ dans le cas contraire.

Puisque le quotient $2a$ se trouve nécessairement dans le développement de $\sqrt{A}$, il s'ensuit donc que l'équation $x^2 - A\,y^2 = \pm 1$ est toujours résoluble (au moins avec le signe $+$), quel que soit le nombre $A$, pourvû qu'il ne soit pas un quarré parfait; et on voit en même temps qu'il y aura une infinité de solntions de cette équation, puisque le quotient $2a$ se répète une infinité de fois dans les périodes successives.

Au reste, si le nombre des termes de la période $\alpha, \mathcal{C} \ldots \mathcal{C}, \alpha, 2a$ est pair, toutes les fractions qui répondent au quotient $2a$ dans les diverses périodes, seront plus grandes que $\sqrt{A}$, et ainsi dans ce cas, ces fractions ne satisferont qu'à l'équation $x^2 - A y^2 = +1$. Mais si le nombre de termes de la période est impair, alors la première fraction qui répond au quotient $2a$ sera plus petite que $\sqrt{A}$, la seconde plus grande, et ainsi alternativement; de sorte que dans ce cas, l'équation $x^2 - A\,y^2 = -1$ sera résoluble aussi bien que l'équation $x^2 - A\,y^2 = +1$, la première par les fractions convergentes de rang impair, la seconde par celles de rang pair.

---

H.

## §. VI. *Résolution en nombres entiers de l'équation indéterminée* $x^2 - Ay^2 = \pm D$, *D étant* $< \sqrt{A}$.

(34) Nous avons fait voir dans le paragraphe précédent, que l'équation $x^2 - Ay^2 = +1$ est toujours résoluble d'une infinité de manières, quel que soit $A$, pourvû qu'il ne soit pas un quarré parfait. Quant à l'équation $x^2 - Ay^2 = -1$, elle n'est résoluble que dans certains cas particuliers; et comme la solution, lorsqu'elle est possible, doit se trouver parmi les fractions convergentes vers $\sqrt{A}$, la condition nécessaire et en même temps suffisante pour la possibilité de cette solution, est que la période de quotiens donnée par le développement de $\sqrt{A}$ soit composée d'un nombre de termes impair.

Les solutions de l'une et l'autre équations se tirent immédiatement des fractions convergentes vers $\sqrt{A}$, savoir de celles qui répondent au quotient $2a$ ($a$ étant l'entier compris dans $\sqrt{A}$), et il y en a une infinité, puisque ce quotient, ainsi que les périodes qui le comprennent, se répète une infinité de fois. Le numérateur de chaque fraction est une valeur de $x$, et son dénominateur, la valeur correspondante de $y$.

Nous ferons voir ci-après comment on trouve *a priori* l'expression générale des diverses fractions qui répondent à un même quotient placé de la même manière dans les périodes successives. Dans le cas présent, il suffit de faire connoître le résultat qui d'ailleurs se vérifie immédiatement.

Soit $\frac{p}{q}$ la première et la plus simple des fractions convergentes qui répondent à un même quotient $2a$; si l'on a $p^2 - Aq^2 = +1$, ou si le nombre des termes de la période est pair, l'équation $x^2 - Ay^2 = +1$ sera, comme nous l'avons déjà dit, la seule résoluble. Pour avoir alors la solution générale, il suffit d'élever

$p+q\sqrt{A}$ à une puissance quelconque $m$, et d'égaler le résultat à $x+y\sqrt{A}$. En effet, si l'on a

$$(p+q\sqrt{A})^m = x+y\sqrt{A},$$

$x$ et $y$ étant rationnels, on aura en même temps

$$(p-q\sqrt{A})^m = x-y\sqrt{A}.$$

Multipliant ces deux équations, le produit sera

$$x^2-Ay^2=(p^2-Aq^2)^m=1^m=1.$$

Donc en effet les valeurs trouvées pour $x$ et $y$ satisferont à l'équation $x^2-Ay^2=1$, quel que soit l'exposant $m$. On peut aussi avoir séparément les valeurs de $x$ et $y$ par les formules

$$x=\frac{(p+q\sqrt{A})^m+(p-q\sqrt{A})^m}{2}$$

$$y=\frac{(p+q\sqrt{A})^m-(p-q\sqrt{A})^m}{2\sqrt{A}}$$

lesquelles donneront toujours des nombres entiers pour $x$ et $y$.

(35) En second lieu, si on a $p^2-Aq^2=-1$, ou si le nombre des termes de la période est impair, alors il est visible qu'on peut satisfaire à-la-fois aux deux équations $x^2-Ay^2=+1$, $x^2-Ay^2=-1$, savoir, à la première, par les puissances paires de $p+q\sqrt{A}$, et à la seconde, par les puissances impaires de ce même binome. Car si l'on fait $(p+q\sqrt{A})^{2k}=x+y\sqrt{A}$, on aura $x^2-Ay^2=(-1)^{2k}=+1$, et si l'on fait $(p+q\sqrt{A})^{2k+1}=x+y\sqrt{A}$, on aura $x^2-Ay^2=(-1)^{2k+1}=-1$.

Par exemple, lorsque $A=13$, on trouve $\frac{p}{q}=\frac{18}{5}$, et $p^2-13q^2=-1$. Donc en faisant $(18+5\sqrt{13})^{2k}=x+y\sqrt{13}$, on satisfera à l'équation $x^2-13y^2=1$, et en faisant $(18+5\sqrt{13})^{2k+1}=x+y\sqrt{13}$, on satisfera à l'équation $x^2-13y^2=-1$.

Les moindres nombres qui satisfont à l'équation $x^2-13y^2=1$, sont donc $x=649$, $y=180$, car on a $(18+5\sqrt{13})^2=649+180\sqrt{13}$.

Quelquefois les nombres les plus simples qui satisfont à une équation donnée $x^2-Ay^2=\pm 1$ sont beaucoup plus considérables. Par exemple, la solution la plus simple de l'équation $x^2-211y^2=1$, est

$$x = 278\ 354\ 373\ 650$$
$$y = 19\ 162\ 705\ 353,$$

et la solution la plus simple de l'équation $x^2 - 56587y^2 = 1$, est

$$x = 166\ 100\ 725\ 257\ 977\ 318\ 398\ 207\ 998\ 462\ 201\ 324\ 702\ 014\ 613\ 503$$
$$y = 698\ 253\ 616\ 416\ 770\ 487\ 157\ 775\ 940\ 222\ 021\ 002\ 391\ 003\ 072.$$

D'où l'on voit combien il est nécessaire d'avoir, pour la recherche de ces nombres, une méthode sûre et infaillible, telle que celle que nous avons exposée; car on se tromperoit beaucoup, si après avoir essayé inutilement la résolution par des nombres médiocrement grands, on concluoit qu'elle n'est possible en aucuns nombres.

(36) Fermat est le premier qui ait paru connoître la résolution de l'équation $x^2 - Ay^2 = 1$, du moins il proposa ce problême comme par défi aux Géomètres anglois, et mylord Brownker en donna une solution qu'on trouve dans les Œuvres de Wallis, et qui est rapportée à-peu-près textuellement dans le second volume de l'algèbre d'Euler. Mais d'un côté, Fermat n'a rien publié sur sa propre solution, et de l'autre, la méthode des Géomètres anglois, quoique fort ingénieuse, n'établit cependant pas d'une manière certaine, que le problême soit toujours possible. Il restoit donc à démontrer, que l'équation $x^2 - Ay^2 = 1$ est toujours résoluble en nombres entiers, et c'est ce que Lagrange a fait d'une manière aussi élégante que solide dans les Mélanges de Turin, tome IV, et ensuite dans les Mémoires de Berlin, ann. 1767; cette démonstration, ainsi que la méthode de solution qui l'accompagne, doivent être regardées comme l'un des plus grands pas qui aient été faits jusqu'à présent dans l'analyse indéterminée. En effet, l'équation $x^2 - Ay^2 = 1$ n'est pas seulement intéressante en elle-même; elle est encore nécessaire dans la résolution de toutes les équations indéterminées du second degré, où elle sert à trouver une infinité de solutions quand on en connoît une seule.

L'importance de cette équation a engagé Euler à donner, dans l'ouvrage cité, une petite table des valeurs les plus simples de $x$ et $y$ pour tous les nombres $A$ depuis 1 jusqu'à 100. Lagrange y a joint, dans ses additions, les quotiens des fractions continues d'où ces valeurs peuvent être tirées.

Ayant eu occasion autrefois de m'occuper de cet objet, même

avant d'avoir connoissance des travaux d'Euler et de Lagrange qui y ont rapport, j'avois calculé une table des plus simples fractions $\frac{m}{n}$ qui satisfont à l'équation $m^2 - A n^2 = \pm 1$, pour tout nombre non quarré $A$ depuis 2 jusqu'à 1003. Cette table pouvant faire plaisir aux amateurs de l'analyse indéterminée, je l'ai jointe à ce Traité. Elle servira à résoudre presque sans calcul toutes les équations $x^2 - A y^2 = \pm D$, dans lesquelles $D$ est $< \sqrt{A}$, et $A < 1004$.

L'inspection seule des chiffres qui terminent les nombres $m$ et $n$ fera voir s'ils satisfont à l'équation $m^2 - A n^2 = +1$, ou à l'équation $m^2 - A n^2 = -1$. Quand ils satisfont à cette dernière, il faut faire $(m + n\sqrt{A})^2 = p + q\sqrt{A}$, afin d'avoir les moindres nombres $p$ et $q$ qui satisfont à l'équation $x^2 - A y^2 = +1$ : on a alors $p = 2m^2 - 1$, $q = 2mn$.

(37) Venons maintenant à la résolution de l'équation proposée $x^2 - A y^2 = \pm D$. On a vu (n°. 10) que lorsque $D$ est $< \sqrt{A}$, comme nous le supposons, la fraction $\frac{x}{y}$ doit être l'une des fractions convergentes vers $\sqrt{A}$. Il faudra donc développer $\sqrt{A}$ en fraction continue, et calculer les valeurs successives des quotiens-complets $\frac{\sqrt{A} + I}{D}$; si parmi ces quotiens-complets, il s'en trouve un dont le dénominateur $D$ soit égal au second membre de l'équation proposée, on en déduira une solution, soit de l'équation $x^2 - A y^2 = +D$, soit de l'équation $x^2 - A y^2 = -D$ : il faudra pour cela calculer la fraction convergente $\frac{p}{q}$ qui répond au quotient-complet dont il s'agit; si cette fraction est de rang impair ($\frac{1}{0}$ étant censée la première), elle sera plus grande que $\sqrt{A}$, et ainsi on aura $p^2 - Aq^2 = +D$; si elle est de rang pair, on aura $p^2 - A q^2 = -D$.

Il peut se trouver plusieurs fois le même nombre $D$ dans la même période, et il se rencontrera toujours au moins deux fois, puisque la période est symmétrique (excepté lorsque le quotient auquel

répond $\frac{p}{q}$ est le terme moyen de la période, abstraction faite de son dernier terme $2a$). On aura alors autant de solutions soit de l'équation $x^2 - Ay^2 = D$, soit de l'équation $x^2 - Ay^2 = -D$, lesquelles auront lieu également dans toutes les autres périodes.

Si on ne rencontre point le nombre $D$ parmi les dénominateurs des quotiens-complets dans la première période, on sera assuré que l'équation $x^2 - Ay^2 = +D$ et l'équation $x^2 - Ay^2 = -D$, ne peuvent se résoudre ni l'une ni l'autre en nombres entiers.

(38) Mais si on a une ou plusieurs solutions données par la première période des quotiens, comme on vient de l'expliquer, on pourra déduire immédiatement de chacune de ces premières solutions, une formule générale qui contienne une infinité d'autres solutions dépendantes de cette première base. Soit $\frac{p}{q}$ la fraction convergente qui donne $p^2 - Aq^2 = D$; soient en même tems $t$ et $u$ des nombres quelconques qui satisfont à l'équation $t^2 - Au^2 = 1$; si on multiplie ces deux équations entr'elles, le produit pourra être mis sous la forme

$$(pt \pm Aqu)^2 - A(pu \pm qt)^2 = D;$$

de sorte que l'équation $x^2 - Ay^2 = D$ sera résolue généralement par les formules

$$x = pt \pm Aqu$$
$$y = pu \pm qt;$$

et quant aux valeurs de $t$ et $u$, nous avons déjà fait voir que si $m$ et $n$ sont les moindres nombres qui satisfont à l'équation $m^2 - An^2 = 1$, et qu'on prenne pour $k$ un entier quelconque, on aura

$$(m + n\sqrt{A})^k = t + u\sqrt{A}.$$

On voit donc qu'en partant de différentes solutions primitives comprises dans la première période, on aura autant de formules générales qui renfermeront chacune une infinité de solutions de l'équation proposée.

D'ailleurs les valeurs que nous venons de donner pour $x$ et $y$ ont également lieu, soit que $D$ soit positif, soit qu'il soit négatif; elles supposent seulement que $D$ a le même signe dans l'équation

particulière $p^2 - Aq^2 = D$, que dans l'équation générale $x^2 - Ay^2 = D$; elles supposent aussi qu'on a $m^2 - A n^2 = +1$.

Si on avoit $m^2 - A n^2 = -1$, alors les formules

$$x = pt \pm Aqu$$
$$y = pu \pm qt$$

donneroient à-la-fois la solution de l'équation $x^2 - Ay^2 = +D$ et celle de l'équation $x^2 - Ay^2 = -D$, l'une en faisant $(m+n\sqrt{A})^{2k} = t + u\sqrt{A}$, l'autre en faisant $(m+n\sqrt{A})^{2k+1} = t + u\sqrt{A}$.

(39) Si on connoît, soit par la table dont nous avons parlé, soit par tout autre moyen, la fraction la plus simple $\frac{m}{n}$ qui satisfait à l'équation $m^2 - A n^2 = \pm 1$, le simple développement de $\frac{m}{n}$ en fraction continue, donnera la période des quotiens qui résulteroient du développement de $\sqrt{A}$. Or sans connoître les quotiens-complets $\frac{\sqrt{A} + I}{D}$ qui répondent à ces quotiens entiers, ni par conséquent leurs dénominateurs, on peut néanmoins distinguer facilement ceux qui répondent à une valeur donnée de $D$. Ces quotiens sont à fort peu près égaux à $\frac{2a}{D}$, $a$ étant l'entier compris dans $\sqrt{A}$. En effet, puisqu'on a (n°. 30) $I = \frac{p - q^2 D}{q}$, il en résulte $\frac{\sqrt{A} + I}{D} = \frac{\frac{p}{q} + \sqrt{A}}{D} - \frac{q^2}{q}$, donc l'entier $\mu$ compris dans $\frac{\sqrt{A} + I}{D}$ est à-peu-près égal à l'entier compris dans $\frac{2a}{D}$.

(40) Par exemple, ayant à résoudre l'équation $x^2 - 61y^2 = 5$, on développera en fraction continue la fraction $\frac{29718}{3805}$ dont les deux termes satisfont à l'équation $m^2 - 61 n^2 = -1$; on trouvera les quotiens et les fractions convergentes comme il suit :

Quotiens 7, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1

Fr. conv. $\frac{1}{0}, \frac{7}{1}, \frac{8}{1}, \frac{39}{5}, \frac{125}{16}, \frac{164}{21}, \frac{453}{58}, \frac{1070}{137}, \frac{1523}{195}, \frac{5639}{722}, \frac{24079}{3083}, \frac{29718}{3805}$

L'entier compris dans $\sqrt{61}$ est 7, et $\frac{2.7}{5}=2+$, je cherche donc 2 parmi les quotiens; je trouve les deux fractions correspondantes $\frac{164}{21}$, $\frac{453}{58}$, dont la première donne $p^2-61q^2=-5$, et la seconde $p^2-61q^2=5$. Donc l'équation proposée $x^2-61y^2=5$ sera résolue au moyen des formules

$$x = 453t \pm 3538u$$
$$y = 453u \pm 58t$$
$$t+u\sqrt{61} = (29718+3805\sqrt{61})^{2k};$$

et elle le sera également par les formules suivantes calculées d'après la première fraction convergente $\frac{164}{21}$:

$$x = 164t \pm 1281u$$
$$y = 164u \pm 21t$$
$$t+u\sqrt{61} = (29718+3805\sqrt{61})^{2k+1}.$$

On résoudroit de la même manière l'équation $x^2-61y^2=-5$, et on voit pourquoi les deux valeurs trouvées pour $\frac{p}{q}$, quoique donnant deux valeurs de $D$ de signes différens, servent néanmoins à résoudre la même équation; c'est parce que la valeur de $\frac{m}{n}$ est telle que $m^2-61n^2=-1$, car dans tous les cas semblables une solution de l'équation $x^2-61y^2=D$, en donne toujours une de l'équation $x^2-61y^2=-D$, et réciproquement.

(41) Nous remarquerons que si $D$, quoique toujours plus petit que $\sqrt{A}$, avoit un facteur quarré $\theta^2$, en sorte qu'on eût $D=\theta^2D'$, alors, outre les solutions trouvées par la méthode précédente, et dans lesquelles $x$ et $y$ sont toujours premiers entr'eux, il pourroit y en avoir d'autres dans lesquelles $x$ et $y$ auroient pour diviseur commun $\theta$. En effet, si d'une autre part on trouve possible la solution de l'équation $x'^2-Ay'^2=D'$, il est clair qu'on en tirera $x=\theta x'$, $y=\theta y'$. Et ainsi il pourra y avoir autant de nouvelles formules de solution, qu'il y a de manières de diviser $D$ par un quarré.

§. VII.

## §. VII. *Théorèmes sur la possibilité de l'équation* $x^2 - Ay^2 = -1$, *2 ou* $-2$, a *étant un nombre premier.*

(42) *Si* a *est un nombre premier de la forme* $4n+1$, *l'équation* $x^2 - ay^2 = -1$ *sera toujours possible en nombres entiers.*

Soient $p$ et $q$ les nombres les plus simples (autres que 1 et 0) qui satisfont à l'équation $p^2 - aq^2 = 1$; $q$ doit être pair, car s'il étoit impair, $q^2$ seroit de la forme $8n+1$, et $aq^2+1$ de la forme $4n+2$ qui ne peut convenir à aucun quarré. Puisque $q$ est pair, faisons $q = 2mn$, $m$ et $n$ étant premiers entre eux, on aura $p^2 - 1 = 4am^2n^2$; mais $p$ étant impair, et par conséquent $p^2-1$ divisible par 8, il faut encore que l'un des deux nombres $m$ et $n$ soit pair et l'autre impair. Supposons $n$ impair, alors l'équation $(p+1)(p-1) = 4am^2n^2$, dans laquelle $p+1$ et $p-1$ ne peuvent avoir que 2 pour commun diviseur, se décomposera nécessairement de l'une de ces quatre manières :

$$(1)\ \begin{matrix} p+1=2am^2 \\ p-1=2n^2 \end{matrix} \quad (2)\ \begin{matrix} p+1=2m^2 \\ p-1=2an^2 \end{matrix} \quad (3)\ \begin{matrix} p+1=2an^2 \\ p-1=2m^2 \end{matrix} \quad (4)\ \begin{matrix} p+1=2n^2 \\ p-1=2am^2 \end{matrix}$$

La seconde et la quatrième combinaison donneroient $1 = m^2 - an^2$ ou $1 = n^2 - am^2$, et ainsi $p$ et $q$ ne seroient pas les nombres les plus simples qui satisfont à l'équation $p^2 - aq^2 = 1$, contre la supposition. Restent donc la première et la troisième qui donnent $-1 = n^2 - am^2$ ou $-1 = m^2 - an^2$. Dans l'un ou l'autre cas, l'équation $x^2 - ay^2 = -1$ est résolue, et ainsi la proposition est démontrée; cependant puisque $m$ est pair et $n$ impair, il est facile de voir que l'équation $n^2 - am^2 = -1$ ne sauroit subsister; il n'y a donc que l'équation $m^2 - an^2 = -1$ qui puisse avoir lieu, et qui existe nécessairement.

*Corollaire.* Il résulte de ce théorême, que lorsque $a$ est un nombre premier de la forme $4n+1$, tout nombre $N$ qui est de la

forme $x^2 - ay^2$ est en même temps de la forme $ay^2 - x^2$. Car puisqu'on peut alors supposer $-1 = m^2 - an^2$, on aura
$$N = (x^2 - ay^2)(an^2 - m^2) = a(my + nx)^2 - (mx + any)^2.$$

(43) *Si* a *est un nombre premier de la forme* $8n + 3$, *l'équation* $x^2 - ay^2 = -2$ *sera toujours possible en nombres entiers.*

Soient $p$ et $q$ les moindres nombres qui satisfont à l'équation $p^2 - aq^2 = 1$; si on suppose d'abord $q$ impair, et qu'on fasse $q = mn$, $m$ et $n$ étant premiers entr'eux, l'équation $p^2 - 1 = aq^2$ ne pourra se décomposer que de l'une de ces deux manières :

$$\left.\begin{matrix} p+1 = am^2 \\ p-1 = n^2 \end{matrix}\right\}(1) \qquad \left.\begin{matrix} p+1 = m^2 \\ p-1 = an^2 \end{matrix}\right\}(2).$$

La seconde combinaison donneroit $2 = m^2 - an^2$, équation impossible, car puisque $m$ et $n$ sont impairs, la quantité $m^2 - an^2$ est de la forme $8k + 1 - (8n + 3)(8h + 1)$, qui se réduit à la forme $8n - 2$ et ne peut être égale à 2. Donc la première combinaison seule est possible, et si elle a lieu, on aura $n^2 - am^2 = -2$.

En second lieu, si $q$ est pair, et qu'on fasse $q = 2mn$, on aura $p^2 - 1 = 4am^2n^2$, et comme $p^2 - 1$ est de la forme $8k$, on voit encore que l'un des nombres $m$ et $n$ doit être pair et l'autre impair; soit $n$ celui-ci, et l'équation précédente où $p+1$ et $p-1$ n'ont que 2 pour diviseur commun, ne pourra se décomposer que de l'une de ces quatre manières :

$$\left.\begin{matrix} p+1 = 2am^2 \\ p-1 = 2n^2 \end{matrix}\right\}(1) \qquad \left.\begin{matrix} p+1 = 2m^2 \\ p-1 = 2an^2 \end{matrix}\right\}(2)$$

$$\left.\begin{matrix} p+1 = 2an^2 \\ p-1 = 2m^2 \end{matrix}\right\}(3) \qquad \left.\begin{matrix} p+1 = 2n^2 \\ p-1 = 2am^2 \end{matrix}\right\}(4)$$

La première combinaison donne $n^2 - am^2 = -1$, ce qui n'est pas possible, car puisque $n$ est impair et $m$ pair, le premier membre est toujours de la forme $4n + 1$.

La seconde combinaison donne $1 = m^2 - an^2$, et ainsi $p$ et $q$ ne seroient pas les nombres les plus simples qui satisfont à l'équation $p^2 - aq^2 = 1$, ce qui est contre la supposition.

La troisième combinaison donne $-1 = m^2 - a n^2$, équation impossible, parce que le second membre est de la forme $4h - (8n+3)(8k+1)$ ou $4i+1$.

Enfin, la quatrième donneroit $1 = n^2 - a m^2$, ce qui ne peut encore s'accorder avec la supposition faite que $p$ et $q$ sont les nombres les plus simples qui satisfont à l'équation $p^2 - aq^2 = 1$.

Donc il n'y a de possible, parmi toutes ces combinaisons, que la première du premier cas, laquelle donne $n^2 - am^2 = -2$, tandis qu'on a $2p = n^2 + a m^2$, et $q = mn$. Cette combinaison a donc lieu nécessairement, et ainsi l'équation $x^2 - a y^2 = -2$, est toujours résoluble.

*Remarquez* qu'étant donnés les deux nombres $n$ et $m$ qui satisfont à l'équation $n^2 - a m^2 = -2$, on en tireroit $p$ et $q$ par l'équation $(n + m\sqrt{a})^2 = 2p + 2q\sqrt{a}$, et réciproquement étant donnés $p$ et $q$, on en tirera $n$ et $m$ par l'équation $\sqrt{(2p + 2q\sqrt{a})} = n + m\sqrt{a}$, ou par les valeurs $n = \sqrt{(p-1)}$, $m = \sqrt{\left(\frac{p+1}{a}\right)}$. On peut remarquer encore que dans le développement de $\sqrt{a}$ en fraction continue, la fraction convergente $\frac{n}{m}$ répondra au quotient moyen de la première période, et ce quotient sera égal au plus grand entier impair compris dans $\sqrt{a}$. Voyez n°. 39.

(44) *Si* a *est un nombre premier de la forme* $8n-1$, *l'équation* $x^2 - a y^2 = 2$ *sera toujours résoluble en nombres entiers.*

Soient toujours $p$ et $q$ les moindres nombres qui satisfont à l'équation $p^2 - a q^2 = 1$, on peut faire $q = mn$ ou $q = 2m'n$, selon que $q$ est impair ou pair, ce qui donnera les quatre décompositions suivantes de l'équation $p^2 - 1 = a q^2$ :

$$\left.\begin{array}{l} p+1 = a m^2 \\ p-1 = n^2 \end{array}\right\} (1) \qquad \left.\begin{array}{l} p+1 = m^2 \\ p-1 = a n^2 \end{array}\right\} (2)$$

$$\left.\begin{array}{l} p+1 = 2 a m'^2 \\ p-1 = 2 n^2 \end{array}\right\} (3) \qquad \left.\begin{array}{l} p+1 = 2 m'^2 \\ p-1 = 2 a n^2 \end{array}\right\} (4).$$

La première donneroit $2 = a m^2 - n^2$, équation qui ne peut subsister, parce que $m$ et $n$ étant impairs, le second membre est

de la forme $(8k-1)(8h+1)-(8l+1)$, laquelle se réduit à $8e-2$, et ne peut être égale à 2.

La troisième donneroit $1=am'^2-n^2$, équation qui ne peut avoir lieu non plus ; car si $m'$ est pair et $n$ impair, le second membre est de la forme $4k-1$; si $m'$ est impair et $n$ pair, il est encore de la forme $4k-1$, et enfin si $m'$ et $n$ sont tous deux impairs (cas qui d'ailleurs ne peut avoir lieu), le second membre seroit pair.

La quatrième combinaison donneroit $1=m'^2-an^2$, ce qui ne peut avoir lieu, puisque $p$ et $q$ sont supposés les moindres nombres qui satisfont à l'équation $x^2-ay^2=1$.

Donc enfin la seconde combinaison est la seule possible et nécessaire ; elle donne $2=m^2-an^2$, et ainsi l'équation proposée $x^2-ay^2=2$ est toujours résoluble.

On a en même temps $2p=m^2+an^2$, $q=mn$, ce qui donne $2p+2q\sqrt{a}=(m+n\sqrt{a})^2$; d'où l'on voit que les valeurs de $m$ et $n$ étant connues, on en conclut celles de $p$ et $q$, et réciproquement étant donnés $p$ et $q$, on en conclura $m$ et $n$ soit par l'équation $\sqrt{(2p+2q\sqrt{a})}=m+n\sqrt{a}$, soit par les formules $m=\sqrt{(p+1)}$, $n=\sqrt{\left(\frac{p-1}{a}\right)}$.

On peut remarquer encore que la fraction $\frac{m}{n}$ répondra au quotient moyen dans la première période qui résulte du développement de $\sqrt{a}$ en fraction continue.

## §. VIII. *Réduction de la formule* $Ly^2 + Myz + Nz^2$ *à l'expression la plus simple.*

(45) Dans cette formule, on suppose que les coefficiens $L, M, N$ sont des nombres donnés (tels cependant qu'ils ne puissent être divisés tous trois par un même nombre); les quantités $y$ et $z$, au contraire, sont des indéterminées auxquelles on peut attribuer toutes les valeurs possibles en nombres entiers positifs et négatifs, avec cette seule restriction que $y$ et $z$ soient premiers entr'eux. Il y aura donc toujours une infinité de nombres représentés par la même formule $Ly^2 + Myz + Nz^2$; mais en général, cette formule est susceptible de différentes formes qui toutes renferment les mêmes nombres, et il s'agit maintenant de déterminer l'expression la plus simple de toutes ces formes.

Nous considérerons d'abord le cas où $M$ est un nombre pair, parce que c'est celui qui présente le plus d'applications, nous indiquerons ensuite les résultats analogues qui ont lieu lorsque $M$ est impair.

Soit donc proposée la formule $py^2 + 2qyz + rz^2$, dans laquelle $p$, $q$, $r$ sont des nombres donnés; si on veut transformer cette formule en une semblable qui n'en diffère que par les coefficiens, il faudra supposer

$$y = fy' + mz'$$
$$z = gy' + nz'$$

$y'$ et $z'$ étant de nouvelles indéterminées. Cela posé, la substitution de ces valeurs donne la transformée $p'y'^2 + 2q'y'z' + r'z'^2$, dont les coefficiens sont

$$p' = pf^2 + 2qfg + rg^2$$
$$q' = pfm + q(fn + gm) + rgn$$
$$r' = pm^2 + 2qmn + rn^2.$$

Or pour que les quantités $f, g, m, n$, ne restreignent pas l'étendue

des indéterminées $y$ et $z$, dans la formule proposée, il faut que les valeurs de $y'$ et $z'$ exprimées en $y$ et $z$, savoir

$$y' = \frac{ny - mz}{fn - mg}, \quad z' = \frac{fz - gy}{fn - mg},$$

soient des entiers, indépendamment de toute valeur particulière de $y$ et de $z$; il faut donc pour cela qu'on ait $fn - mg = \pm 1$. De-là on voit qu'on peut prendre arbitrairement deux coefficiens tels que $f$ et $g$, pourvu qu'ils soient premiers entr'eux, ensuite on prendra pour $\frac{m}{n}$ la fraction convergente qui précède $\frac{f}{g}$ dans le développement de celle-ci en fraction continue; par ce moyen, la condition $fn - mg = \pm 1$ sera remplie, et on aura la certitude que tout nombre compris dans la formule $py^2 + 2qyz + rz^2$, l'est également dans sa transformée $p'y'^2 + 2q'y'z' + r'z'^2$, et réciproquement. D'ailleurs ayant supposé $y$ et $z$ premiers entr'eux, il faudra que $y'$ et $z'$ le soient aussi, car si $y'$ et $z'$ avoient un commun diviseur $\theta$, les nombres $y$ et $z$ (d'après les valeurs $y = fy' + mz'$, $z = gy' + nz'$) seroient aussi divisibles par $\theta$; ce qui est contre la supposition.

Nous observerons de plus, que les valeurs trouvées pour $p', q', r'$ donnent $p'r' - q'q' = (pr - qq)(fn - mg)^2 = pr - qq$; d'où il suit que *la quantité* pr — qq *et son analogue* p'r' — q'q' *dans la transformée, sont égales et de même signe.*

Cette quantité $pr - q^2$ est celle qui détermine la nature de la formule $py^2 + 2qyz + rz^2$, eu égard aux deux facteurs $\alpha y + \mathcal{C} z$, $\gamma y + \delta z$ dont on peut imaginer qu'elle est composée. Si ces facteurs sont imaginaires, la quantité $pr - q^2$ sera positive : s'ils sont ou égaux, ou rationnels, la quantité $pr - q^2$ sera égale à zéro, ou à un quarré négatif : enfin s'ils sont réels, mais irrationnels, la quantité $pr - q^2$ sera égale à un nombre négatif et non quarré. C'est ce qui se voit, en mettant la formule $py^2 + 2qyz + rz^2$ sous la forme

$$\frac{1}{p}\left[py + qz + z\sqrt{(q^2 - pr)}\right]\left[py + qz - z\sqrt{(q^2 - pr)}\right].$$

Nous examinerons séparément ces différens cas ; mais il faut, avant tout, résoudre le problème général qui suit (1).

(46) *Étant donnée la formule indéterminée* $py^2+2qyz+rz^2$, *dans laquelle le coefficient moyen* $2q$ *excède l'un ou l'autre des coefficiens extrêmes* p *et* r, *ou tous les deux, transformer cette formule en une formule semblable où le coefficient moyen soit moindre que chacun des extrêmes, ou au moins n'excède pas le plus petit des deux.*

Supposons $2q>p$, et dans le cas où l'on auroit à-la-fois $2q>p$, et $2q>r$, soit $p$ le moindre des deux nombres $p$ et $r$, abstraction faite de leurs signes ; nous ferons $y=y'-mz$, $m$ étant un coefficient indéterminé, et la substitution donnera cette transformée

$$py'y'-(2pm-2q)y'z+(pm^2-2qm+r)z^2.$$

Or on peut prendre l'indéterminée $m$, de manière que $2pm-2q$ soit plus petit que $p$, ou égal à $p$ ; il faut pour cela que $m$ soit l'entier le plus proche en plus ou en moins de la fraction donnée $\frac{p}{q}$. Cela posé, faisant $pm-q=q'$, $pm^2-2qm+r=r'$, la transformée sera

$$py'y'-2q'y'z\pm r'z^2,$$

et l'on aura $pr'-q'q'=pr-q^2$, et $2q'<p$, le signe $<$ n'excluant pas l'égalité.

Puisqu'on a à-la-fois $2q>p$ et $2q'<p$, il s'ensuit qu'on aura $q'<q$, ce qui est l'objet principal de cette première opération. Maintenant si dans cette transformée le coefficient $2q'$, quoique $<p$ est encore $>r'$, on procédera semblablement, et on obtiendra une nouvelle transformée dans laquelle le coefficient moyen que j'appelle $2q''$ sera $<2q'$. Or une suite de nombres entiers décroissans $q$, $q'$, $q''$, $q'''$, &c. ne sauroit aller à l'infini : ainsi en continuant les mêmes opérations, on parviendra nécessairement à une transformée dans laquelle il n'y aura plus lieu à réduction ultérieure, et qui sera par conséquent telle, que le coefficient

(1) La solution de ce problème, l'un des plus importans de l'analyse indéterminée, est due à Lagrange. Voyez les Mémoires de Berlin, année 1773.

moyen ne surpasse aucun des extrêmes. Cette transformée satisfera au problême proposé; ses indéterminées seront encore des nombres premiers entr'eux, et la quantité analogue à $pr-q^2$ sera de même valeur et de même signe que dans la formule proposée; car ces deux conditions sont toujours observées dans le passage d'une transformée à l'autre, comme nous l'avons démontré.

Soit prise pour exemple la formule $35y^2+172yz+210z^2$; comme l'entier le plus proche de $\frac{q}{p}=\frac{86}{35}$ est 2, on fera $y=y'-2z$, ce qui donnera la transformée

$$\begin{array}{l}35y'y'-140y'z+140z^2=35y'y'+32y'z+6z^2\\ \quad+172\quad-344\\ \qquad\qquad+210.\end{array}$$

Dans celle-ci, le coefficient moyen 32 étant plus grand que l'extrême 6, il faut procéder de la même manière à une nouvelle transformation. Prenant donc l'entier le plus proche de $\frac{16}{6}$ qui est 3, on fera $z=z'-3y'$, et la seconde transformée sera

$$\begin{array}{l}6z'z'-36z'y'+54y'y'=6z'z'-4z'y'-7y'y'\\ \quad+32\quad-96\\ \qquad\qquad+35.\end{array}$$

Cette dernière a les conditions requises, puisque le coefficient moyen 4 est moindre que chacun des extrêmes 6 et 7. En même temps, on voit que la quantité $pr-q^2$ est $-46$ dans la formule proposée comme dans sa dernière transformée; et quant à la relation des premières variables $y$ et $z$, avec les nouvelles $y'$ et $z'$, on trouve qu'elle est donnée par les équations

$$y=7y'-2z'$$
$$z=z'-3y'.$$

Examinons maintenant les trois cas généraux dont nous avons fait mention ci-dessus (n°. 45).

(47) Soit 1°. $pr-q^2$ égal à un nombre négatif $-A$, nous pourrons supposer que la formule $py^2+2qyz+rz^2$ est réduite à la forme la plus simple, en sorte que $2q$ n'excède ni $p$ ni $r$; mais alors je

je dis que les nombres $p$ et $r$ sont de signes différens ; car s'ils avoient le même signe, $pr$ seroit positif et $> 4q^2$, donc $pr - q^2$ seroit positif et $> 3q^2$, quantité qui ne pourroit être égale à $-A$. Nous pouvons donc supposer que la formule dont il s'agit est $ay^2 + 2byz - cz^2$, où l'on aura $a$ et $c$ positifs, et $ac + b^2 = A$. Mais d'ailleurs on a toujours $2b < a$ et $c$, et par conséquent $ac + b^2 > 5b^2$, donc on a $5b^2 < A$, ou $b < \sqrt{\frac{A}{5}}$; en même temps les limites de $ac$ sont $ac < A$, $ac > \frac{4}{5}A$.

*Remarque.* Il peut arriver que différentes formules, telles que $ay^2 + 2byz - cz^2$ répondent à une même valeur de $A$, et satisfassent à la condition $2b < a$ et $c$, sans cependant différer essentiellement entr'elles. Par exemple, les deux formules $y^2 - 7z^2$ et $2y^2 + 2yz - 3z^2$ donnent également $ac + b^2 = 7$, et $2b < a$ et $c$; cependant si l'on fait $y = 2t - 5u$, $z = 3u - t$, la formule $2y^2 + 2yz - 3z^2$ deviendra $t^2 - 7u^2$; et réciproquement, si dans cette dernière on fait $t = 3y + 5z$, $u = y + 2z$, elle se réduit à la première $2y^2 + 2yz - 3z^2$. D'où l'on voit que ces deux formules ne sont réellement que deux expressions différentes d'une seule et même formule, et qu'il n'est aucun nombre contenu dans l'une qui ne soit également contenu dans l'autre avec la même valeur et le même signe.

Le nombre $A$ étant donné, il est facile de trouver toutes les formules $ay^2 + 2byz - cz^2$ qui satisfont aux conditions $b^2 + ac = A$, $2b < a$ et $c$; et il est clair que le nombre de ces formules est nécessairement limité, puisqu'on doit avoir $a$ et $c$ positifs, et $b < \sqrt{\frac{A}{5}}$. Mais après avoir trouvé ces diverses formules, il restera à distinguer celles qui ne diffèrent point essentiellement entre elles, afin qu'on soit en état de réduire la totalité au plus petit nombre possible. Nous nous occuperons de cette recherche dans le §. XIII.

2°. Si en supposant toujours $pr - q^2 = -A$, $A$ est un quarré parfait, alors la formule proposée $py^2 + 2qyz + rz^2$ sera décomposable en deux facteurs rationnels $(\alpha y + \beta z)(\gamma y + \delta z)$; si de plus on a $pr - q^2 = 0$, ces deux facteurs seront égaux. Ces cas

n'ont pas besoin d'un plus grand développement, et on voit facilement quelle seroit alors l'expression la plus simple de la formule proposée.

Soit donc 3°. $pr-q^2=$ à un nombre positif $A$, et supposons de nouveau que la formule $py^2+2qyz+rz^2$ soit réduite à son expression la plus simple, de sorte que $2q$ ne surpasse ni $p$ ni $r$. Alors on aura $pr>4q^2$ et $3q^2<A$, ou $q<\sqrt{\frac{A}{3}}$; en même temps on voit que $pr$ sera toujours compris entre $A$ et $\frac{4}{3}A$.

Étant donné le nombre $A$, il est facile de trouver toutes les formules $py^2+2qyz+rz^2$ qui satisfont aux conditions $pr-q^2=A$, et $2q<p$ et $r$. On peut démontrer de plus, que toutes ces formules sont essentiellement différentes les unes des autres, et ne peuvent se réduire à un moindre nombre. Ce sera l'objet des deux propositions suivantes.

(48) THÉORÈME. *Si la formule indéterminée* $py^2+2qyz+rz^2$ *est telle que* $2q$ *ne surpasse ni* $p$ *ni* $r$; *si en même temps* $pr-q^2$ *est égal à un nombre positif* $A$, *je dis que les deux plus petits nombres compris dans cette formule sont* $p$ *et* $r$.

On observera d'abord que la formule $py^2+2qyz+rz^2$, considérée analytiquement, est la même que $py^2-2qyz+rz^2$, parce qu'on peut faire à volonté les indéterminées $y$ et $z$ positives ou négatives. Or toutes choses d'ailleurs égales, la formule $py^2+2qyz+rz^2$ dont nous supposerons les trois termes positifs, est plus grande que la formule $py^2-2qyz+rz^2$; ainsi ce n'est qu'à l'égard de cette dernière que le *minimum* peut avoir lieu.

Soit donc $P=py^2-2qyz+rz^2$, et soit $y>z$. Mettons $y-1$ à la place de $y$, et supposons que $P$ devienne $P'$, nous aurons

$$P'=P-2py+p+2qz$$

$$\text{ou } P'=P-2q(y-z)-y(p-2q)-p(y-1).$$

Or à cause de $p>2q$ et $y>z$, il est manifeste que $P'$ est moindre que $P$, quand même le signe $>$ comprendroit l'égalité, comme on le suppose toujours.

On pourroit objecter que quoiqu'on ait $P'=P-Q.$, $Q$ étant

une quantité positive, cependant si $Q$ est lui-même plus grand que $P$, alors $P'$ pourroit avoir une valeur négative plus grande que $P$. Mais cette objection tombe d'elle-même, en observant qu'il n'y a aucune valeur de $y$ et de $z$ qui puisse rendre la formule $py^2-2qyz+rz^2$ négative, attendu que ses facteurs sont imaginaires.

Il suit de-là que, quelles que soient les valeurs de $y$ et $z$ qui donnent le résultat $P$, on trouvera un résultat moindre en diminuant d'une unité la plus grande des deux quantités $y$ et $z$, ou l'une des deux, si elles sont égales; car la conclusion qu'on a tirée auroit également lieu, si on avoit $y=z$. Mais en continuant ainsi à diminuer les indéterminées $y$ et $z$, on parviendra nécessairement aux valeurs $y=1$, $z=1$; donc la quantité $P=p-2q+r$ qui répond aux valeurs $y=1$, $z=1$, est plus petite que toutes celles qui répondent à des valeurs plus grandes de ces variables.

D'un autre côté, puisque $2q$ est $<p$ et $r$, la quantité $p-2q+r$ est plus grande, ou au moins égale à la plus grande des quantités $p$ et $r$. Donc ces deux nombres $p$ et $r$ sont les plus petits qui soient compris dans la formule proposée, et après ceux-ci le plus petit est $p-2q+r$.

(49) Théorème. *Si deux formules indéterminées* $py^2+2qyz+rz^2$, $p'y^2+2q'yz+r'z^2$, *sont telles l'une et l'autre, que le coefficient du terme moyen ne surpasse aucun des coefficiens extrêmes ; si en même temps les quantités* $pr-q^2$, $p'r'-q'^2$ *sont égales à un même nombre positif* $A$, *je dis que ces deux formules sont essentiellement différentes l'une de l'autre, et qu'elles ne peuvent se réduire à une même formule.*

Car s'il étoit possible de transformer l'une de ces formules dans l'autre, il faudroit que l'une des deux renfermât au moins un nombre moindre que ses coefficiens extrêmes, ce qui est contre le théorême précédent.

(50) Jusqu'à présent, nous n'avons considéré la formule $Ly^2+Myz+Nz^2$ que dans le cas où le coefficient moyen $M$ est pair. Supposons maintenant que ce coefficient soit impair, on trou-

vera, par des considérations semblables, les résultats suivans qu'il nous suffit d'indiquer.

1°. Toute formule indéterminée $Ly^2+Myz+Nz^2$ dans laquelle on a $M>2L$, peut se réduire à nne formule semblable dans laquelle le coefficient moyen sera moindre que $2L$, et où la quantité analogue à $4LN-M^2$ sera de même valeur et de même signe. Il faut pour cela faire $y=y'-mz$, et prendre pour $m$ l'entier le plus approché de $\frac{M}{2L}$.

2°. Donc par une ou plusieurs transformations de cette sorte, on changera la formule proposée en une formule semblable, dans laquelle le coefficient du terme moyen ne surpassera aucun des extrêmes, et où la quantité $4LN-M^2$ sera de même valeur et de même signe que dans la proposée.

3°. Lorsque $4LN-M^2$ est égal à un nombre négatif $-B$, la transformée qui satisfait aux conditions précédentes est de la forme $ay^2+byz-cz^2$, dans laquelle on a $B=b^2+4ac$, $b<a$ et $c$, et par conséquent $b<\sqrt{\frac{B}{5}}$.

Étant donné le nombre $B$, on peut trouver aisément toutes les formules $ay^2+byz-cz^2$ qui satisfont aux conditions $b^2+4ac=B$, $b<a$ et $c$. Mais plusieurs de ces formules peuvent être identiques ou transformables les unes dans les autres; c'est ce qu'on examinera dans le §. XIII.

4°. Lorsqne $4LN-M^2$ est égal à un nombre positif $B$, la transformée $ay^2+byz+cz^2$ qui satisfait aux conditions précitées $4ac-b^2=B$, $b<a$ et $c$, et par conséquent $b<\sqrt{\frac{B}{3}}$, est telle qne $a$ et $c$ sont les deux plus petits nombres qui y soient compris.

Donc toutes les formules de cette sorte qui répondent à un même nombre donné $B$, sont essentiellement différentes les unes des autres, et ne peuvent se réduire à un plus petit nombre.

## §. IX. *Développement de la racine d'une équation du second degré en fraction continue.*

(51) Soit $fx^2+gx+h=0$ une équation proposée, dont les coefficiens sont entiers et les racines réelles; on propose de développer en fraction continue l'une de ces racines, que pour plus de simplicité on regardera comme positive (si elle étoit négative, on mettroit $-x$ à la place de $x$, et on feroit précéder le résultat du signe $-$).

Ayant commencé l'opération d'après la méthode générale, supposons qu'on soit parvenu aux deux fractions convergentes consécutives $\frac{p^\circ}{q^\circ}$, $\frac{p}{q}$, et soit $z$ le quotient-complet qui répond à la dernière, on aura $x=\frac{pz+p^\circ}{qz+q^\circ}$, et par conséquent $z=\frac{q^\circ x-p^\circ}{p-qx}$. Substituant au lieu de $x$ sa valeur $x=\frac{-g+\sqrt{(g^2-4fh)}}{2f}$, on aura

$$z=\frac{-gq^\circ-2fp^\circ+q^\circ\sqrt{(g^2-4fh)}}{gq+2fp-q\sqrt{(g^2-4fh)}};$$

quantité qui, en rendant le dénominateur rationnel, devient

$$z=\frac{\frac{1}{2}(pq^\circ-p^\circ q)\sqrt{(g^2-4fh)}-fpp^\circ-\frac{1}{2}g(pq^\circ+p^\circ q)-hqq^\circ}{fp^2+gpq+hq^2}.$$

Si pour abréger, on représente cette valeur par la formule $z=\frac{\sqrt{A}+I}{D}$, les quantités $A$, $I$, $D$, seront exprimées comme il suit:

$$A=\tfrac{1}{4}(g^2-4fh)$$

$$(pq^\circ-p^\circ q)\,I=-fpp^\circ-\tfrac{1}{2}g(pq^\circ+p^\circ q)-hqq^\circ$$

$$(pq^\circ-p^\circ q)\,D=fp^2+gpq+hq^2,$$

où l'on voit qu'à cause de $pq^\circ-p^\circ q=\pm1$, le nombre $D$ sera toujours un entier; quant au nombre $I$, il sera entier, si $g$ est pair; mais il contiendra toujours la fraction $\frac{1}{2}$, si $g$ est impair.

(52) Quelque loin qu'on ait poussé le développement de $x$ en fraction continue, on voit que le quotient-complet $z$ s'exprime facilement au moyen des deux dernières fractions convergentes $\frac{p^0}{q^0}$, $\frac{p}{q}$, ce qui pourroit servir à continuer le développement encore plus loin. Mais indépendamment des fractions convergentes, on peut avoir la loi de progression des quotiens-complets ; en effet, soient

$$\frac{\sqrt{A}+I^0}{D^0}, \quad \frac{\sqrt{A}+I}{D}, \quad \frac{\sqrt{A}+I'}{D'}$$

trois de ces quotiens consécutifs ; et soient $\frac{p^0}{q^0}$, $\frac{p}{q}$, $\frac{p'}{q'}$ les fractions convergentes qui leur correspondent : si on fait pour abréger $pq^0 - p^0q = i$, on aura, comme nous venons de le trouver,

$$iI = -fpp^0 - \tfrac{1}{2}g(pq^0 + p^0q) - hqq^0$$
$$iD = fp^2 + gpq + hq^2.$$

Passant de-là aux valeurs suivantes, et observant qu'alors $i$ change de signe, parce qu'on a $p'q - pq' = -(pq^0 - p^0q)$, ces formules deviendront

$$-iI' = -fp'p - \tfrac{1}{2}g(p'q + pq') - hq'q$$
$$-iD' = fp'p' + gp'q' + hq'q'.$$

Or si on appelle à l'ordinaire $\mu$ le quotient qui répond à la fraction $\frac{p}{q}$, on aura $p' = \mu p + p^0$, $q' = \mu q + q^0$, valeurs qui étant substituées dans la première équation, donneront

$$iI' = \mu(fp^2 + gpq + hq^2) + fpp^0 + \tfrac{1}{2}g(pq^0 + p^0q) + hqq^0,$$

ou $iI' = \mu iD - iI$, de sorte qu'on a sans ambiguité

$$I' = \mu D - I.$$

Faisant les mêmes substitutions dans l'équation en $D$, on aura pareillement

$$-D'i = \mu^2(fp^2 + gpq + hq^2) + \mu(2fpp^0 + gp^0q + gpq^0 + 2hqq^0)$$
$$+ fp^{02} + gp^0q^0 + hq^{02};$$

et le second membre se réduisant à $\mu^2 Di - 2\mu Ii - iD^0$, on aura encore sans ambiguité

$$D' = D^0 + 2\mu I - \mu^2 D;$$

ou $D'=D^{\circ}+\mu\,(I-I')$. De-là il suit qu'étant donnés deux quotiens-complets consécutifs

$$\frac{\sqrt{A}+I^{\circ}}{D^{\circ}}=\mu^{\circ}+$$

$$\frac{\sqrt{A}+I}{D}=\mu+$$

le suivant $\dfrac{\sqrt{A}+I'}{D'}$ se déterminera très-simplement par les valeurs

$$I'=\mu D-I$$
$$D'=D^{\circ}+\mu(I-I');$$

ce qui est la même loi qu'on a trouvée (n°. 29) dans le développement des racines quarrées.

(53) Si on élimine $\mu$ des deux formules précédentes, on aura $D'D+I'^2=DD^{\circ}+I^2$; mais le premier membre de cette équation renferme les mêmes quantités que le second, avec la seule différence qu'elles sont avancées d'un rang de plus; il s'ensuit donc que chaque membre est une quantité constante. Pour déterminer cette quantité en fonction des coefficiens de l'équation proposée, soit $k$ l'entier le plus grand compris dans $x$, le développement de la valeur de $x$ commencera ainsi:

$$x=\frac{\sqrt{A}-\frac{1}{2}g}{f}=k+\frac{\sqrt{A}-\frac{1}{2}g-fk}{f}$$

$$\frac{f}{\sqrt{A}-\frac{1}{2}g-fk}=\frac{\sqrt{A}+\frac{1}{2}g+fk}{-fk^2-gk-h}=\text{\&c.}$$

Donc à l'égard des deux premiers quotiens-complets, on peut supposer $D^{\circ}=f$, $D=-fk^2-gk-h$, $I=\frac{1}{2}g+fk$, ce qui donnera $D^{\circ}D+I^2=\frac{1}{4}g^2-fh=A$. Donc quel que soit le rang du quotient-complet $\dfrac{\sqrt{A}+I}{D}$, on aura généralement

$$D^{\circ}D+I^2=A.$$

Il pourra arriver que les premières valeurs de $D$ soient alternativement positives et négatives; car quoique $x$ soit toujours compris entre deux fractions convergentes consécutives $\dfrac{p^{\circ}}{q^{\circ}}$, $\dfrac{p}{q}$, cependant si les deux racines de l'équation $fx^2+gx+h=0$ diffèrent

moins entr'elles que ne diffèrent l'une de l'autre ces deux fractions convergentes, il est facile de voir que les deux résultats

$$fp^{\circ 2}+gp^{\circ}q^{\circ}+hq^{\circ 2}$$
$$fp^2+gpq+hq^2,$$

obtenus en substituant, dans le premier membre de l'équation $\frac{p^{\circ}}{q^{\circ}}$ et $\frac{p}{q}$ à la place de $x$, seront nécessairement de même signe; donc alors $D^{\circ}$ et $D$ seront de signes différens. Mais comme l'approximation augmente rapidement à l'aide des fractions continues, cette alternation de signes ne peut avoir lieu que dans un petit nombre des premiers termes, et bientôt après les quantités $D$ seront constamment de même signe.

A compter de cette époque, où la série des quotiens-complets prend une forme plus régulière, la quantité $DD^{\circ}$ étant toujours positive, on aura à-la-fois $I<\sqrt{A}$ et $D<2\sqrt{A}$. Les valeurs de $I$ et de $D$ étant ainsi limitées, et d'ailleurs les nombres $2I$ et $D$ étant toujours des entiers, le quotient-complet $\frac{\sqrt{A}+I}{D}$ ne peut avoir qu'un certain nombre de valeurs différentes. Donc après un nombre de termes plus ou moins grand, mais qui ne peut excéder $\sqrt{A}\times 2\sqrt{A}$, on retombera nécessairement sur un quotient-complet déjà trouvé, après quoi le reste de la fraction continue ne sera plus composé que d'une même série ou période de quotiens déjà trouvés, laquelle se répétera à l'infini.

(54) Cela posé, il y aura une infinité de fractions convergentes $\frac{p}{q}$, $\frac{p1}{q1}$, $\frac{p2}{q2}$, &c. qui dans les périodes successives répondront à un même quotient-complet $\frac{\sqrt{A}+I}{D}$; et il est d'autant plus important de rechercher l'expression générale de ces fractions, qu'elles serviront à donner une infinité de solutions des équations de la forme $fy^2+gyz+hz^2=\pm D$.

Soit donc $\mu$, $\mu'$, $\mu''$ ...... $\omega$ la période de quotiens qui, répétée une infinité de fois, forme le développement de $\frac{\sqrt{A}+I}{D}$; au moyen de

de ces quotiens, on continuera ainsi le calcul des fractions convergentes vers $x$ :

Quotiens... $\mu$, $\mu'$ ........ $\omega$, $\mu$, $\mu'$ ...... $\omega$, $\mu$, $\mu'$....

Fract. conv. $\frac{p^\circ}{q^\circ}$, $\frac{p}{q}$, $\frac{p'}{q'}$..... $\frac{p^\circ 1}{q^\circ 1}$, $\frac{p1}{q1}$...... $\frac{p^\circ 2}{q^\circ 2}$, $\frac{p2}{q2}$......

Représentons en outre par $\frac{\alpha}{\zeta}$ la valeur de la fraction continue $\mu+\frac{1}{\mu'+\frac{1}{\mu''\ \&c.}}$ calculée jusqu'au terme $\omega$ inclusivement. Cela posé, de même qu'on a, quel que soit $\mu$, $\frac{p'}{q'}=\frac{p\mu+p^\circ}{q\mu+q^\circ}$; de même, en mettant $\frac{\alpha}{\zeta}$ au lieu de $\mu$, on aura

$$\frac{p1}{q1}=\frac{p\frac{\alpha}{\zeta}+p^\circ}{q\frac{\alpha}{\zeta}+q^\circ}=\frac{p\alpha+p^\circ\zeta}{q\alpha+q^\circ\zeta},$$

ce qui donne $p1=p\alpha+p^\circ\zeta$, $q1=q\alpha+q^\circ\zeta$. On auroit aussi, en mettant $\frac{\sqrt{A}+I}{D}$ à la place de $\mu$,

$$x=\frac{p\left(\frac{\sqrt{A}+I}{D}\right)+p^\circ}{q\left(\frac{\sqrt{A}+I}{D}\right)+q^\circ}=\frac{p\sqrt{A}+pI+p^\circ D}{q\sqrt{A}+qI+q^\circ D}=\frac{\sqrt{A}-\frac{1}{2}g}{f}.$$

Cette équation donneroit les mêmes valeurs de $I$ et $D$ qu'on a trouvées ci-dessus ; on en tire aussi immédiatement

$$p^\circ=-\frac{p}{D}(\tfrac{1}{2}g+I)-\frac{hq}{D}$$

$$q^\circ=\frac{q}{D}(\tfrac{1}{2}g-I)+\frac{fp}{D}.$$

Substituant ces valeurs dans celles de $p1$ et $q1$, il en résultera

$$p1=p\left(\alpha-\frac{\zeta}{D}I-\frac{\zeta}{D}\cdot\tfrac{1}{2}g\right)-\frac{\zeta}{D}hq$$

$$q1=q\left(\alpha-\frac{\zeta}{D}I+\frac{\zeta}{D}\cdot\tfrac{1}{2}g\right)+\frac{\zeta}{D}fp.$$

On aura donc semblablement, à cause de l'égalité des périodes,

$$p2 = p1\left(\alpha - \frac{c}{D}I - \frac{c}{D}\cdot\tfrac{1}{2}g\right) - \frac{c}{D}hq1$$

$$q2 = q1\left(\alpha - \frac{c}{D}I + \frac{c}{D}\cdot\tfrac{1}{2}g\right) + \frac{c}{D}fp1.$$

Soit pour abréger $\alpha - \frac{c}{D}I = \varphi$, $\frac{c}{D} = \psi$, $\varphi^2 - A\psi^2 = \epsilon$, on tirera de ces équations

$$p2 = 2\varphi p1 - \epsilon p$$
$$q2 = 2\varphi q1 - \epsilon q.$$

D'où il suit que les numérateurs $p$, $p1$, $p2$, &c. forment une suite récurrente dont l'échelle de relation est $2\varphi$, $-\epsilon$: il en est de même de la série des dénominateurs $q$, $q1$, $q2$, &c. Et ce résultat est applicable non-seulement aux trois premiers termes $\frac{p}{q}$, $\frac{p1}{q1}$, $\frac{p2}{q2}$; mais à trois autres quelconques, pourvû qu'ils se suivent immédiatement.

Or il résulte de la théorie connue de ces suites, que si l'on fait

$$(\varphi + \psi\sqrt{A})^n = \Phi + \Psi\sqrt{A},$$

$n$ étant un entier quelconque, le terme général demandé $\frac{p_n}{q_n}$ sera donné par les formules

$$p_n = a'\Phi + b'\Psi$$
$$q_n = a''\Phi + b''\Psi,$$

où il ne reste plus à déterminer que les coefficiens $a'$, $b'$, $a''$, $b''$. Pour cela, soit $n=0$, et conséquemment $\Phi=1$, $\Psi=0$, on pourra supposer $p_n = p$, $q_n = q$, et ainsi on aura $a' = p$, $a'' = q$; soit ensuite $n=1$, il faudra qu'on ait

$$p1 = p\varphi + b'\psi$$
$$q1 = q\varphi + b''\psi;$$

de-là et des valeurs connues de $p1$ et $q1$, on tire

$$b' = -\tfrac{1}{2}gp - hq$$
$$b'' = \tfrac{1}{2}gq + fq.$$

Donc enfin le terme général $\frac{p_n}{q_n}$ sera déterminé par les formules

$$p_n = p\Phi - (\tfrac{1}{2}gp + hq)\Psi$$
$$q_n = q\Phi + (\tfrac{1}{2}gq + fp)\Psi.$$

Nous allons maintenant faire voir que, quoique les valeurs de $\varphi$ et $\psi$, et par conséquent celles de $\Phi$ et $\Psi$ paroissent se présenter sous une forme fractionnaire, cependant ces quantités ne peuvent contenir au plus que la fraction $\frac{1}{2}$, ce qui n'empêchera pas les valeurs de $p_n$ et $q_n$ d'être toujours des entiers.

(55) Considérons la fraction continue qui résulte du quotient-complet $z = \frac{\sqrt{A}+I}{D}$, et qui est composée, comme nous l'avons déjà dit, de la période $\mu$, $\mu'$, $\mu''$... $\omega$ répétée une infinité de fois; si on calcule les fractions convergentes vers $z$, par la loi ordinaire.

Quotiens..... $\mu$, $\mu'$, $\mu''$........ $\omega$, $\mu$, $\mu'$, $\mu''$....... $\omega$, &c.
Fract. converg. $\frac{1}{0}$, $\frac{\mu}{1}$, .......... $\frac{\alpha^0}{\beta^0}$, $\frac{\alpha}{\beta}$.......

On aura, après la première période, $z = \frac{\alpha z + \alpha^0}{\beta z + \beta^0}$, ou $\beta z^2 + (\beta^0 - \alpha) z = \alpha^0$. Substituant, au lieu de $z$, sa valeur $\frac{\sqrt{A}+I}{D}$, et égalant entr'eux les termes de la même espèce, on aura les deux équations

$$\beta\left(\frac{A+I^2}{D^2}\right) + (\beta^0 - \alpha)\frac{I}{D} = \alpha^0$$

$$\beta \cdot \frac{2I}{D^2} + \frac{\beta^0 - \alpha}{D} = 0;$$

d'où l'on tire $\frac{\beta I}{D} = \frac{\alpha - \beta^0}{2}$, et $\alpha^0 = \beta\left(\frac{A - I^2}{D^2}\right) = \frac{\beta D^0}{D}$. Maintenant les valeurs de $\varphi$ et $\psi$ donnent

$$\varphi^2 - A\psi^2 = \alpha^2 - \frac{2\alpha\beta}{D} I + \frac{\beta^2}{D^2} I^2 - \frac{\beta^2}{D^2} A;$$

Et d'abord, à cause de $A - I^2 = DD^0$, le second membre se réduit à $\alpha^2 - \frac{2\alpha\beta}{D} I - \frac{\beta^2}{D} D^0$; ensuite si on substitue les valeurs trouvées de $\frac{\beta I}{D}$ et $\frac{\beta D^0}{D}$, il devient $\alpha^2 - 2\alpha\left(\frac{\alpha - \beta^0}{2}\right) - \beta\alpha^0$, ou $\alpha\beta^0 - \alpha^0\beta = \pm 1$, de sorte qu'on a

$$\varphi^2 - A\psi^2 = \pm 1.$$

Il paroît, par ce résultat, que les quantités $\varphi$ et $\psi$ sont les mêmes, soit que la période $\mu, \mu', \mu'' \ldots \omega$ commence au quotient $\mu$, ou à tout autre terme $\mu', \mu''$, &c., pourvu qu'elle soit composée des mêmes quotiens disposés dans l'ordre de la période; et c'est d'ailleurs ce dont il est facile de s'assurer, en prenant $I'$ et $D'$ au lieu de $I$ et $D$, et calculant une valeur de $\frac{\alpha}{\zeta}$ qui réponde aux quotiens $\mu', \mu'' \ldots \omega, \mu$; car il en résultera absolument les mêmes valeurs pour les nombres $\varphi$ et $\psi$.

Au reste, puisqu'on a $\varphi = \alpha - \frac{\zeta}{D} I = \frac{\alpha + \zeta^{\circ}}{2}$, il est clair que le nombre $\varphi$ est entier, ou ne contient au plus que la fraction $\frac{1}{2}$; quant à l'autre nombre $\psi = \frac{\zeta}{D}$, je dis qu'il est toujours un entier.

(56) En effet, si $\frac{\zeta}{D}$ n'est pas un entier, soit $\frac{\gamma}{\delta}$ son expression la plus simple, en sorte qu'on ait $\zeta = \theta\gamma$, $D = \theta\delta$; nous avons trouvé $\frac{\alpha^{\circ}}{D^{\circ}} = \frac{\zeta}{D} = \frac{\gamma}{\delta}$, on pourra donc faire aussi $\alpha^{\circ} = \lambda\gamma$, $D^{\circ} = \lambda\delta$. On a d'ailleurs $\frac{\zeta I}{D} = \frac{\gamma I}{\delta} = \frac{\alpha - \zeta^{\circ}}{2}$; donc $\frac{\alpha - \zeta^{\circ}}{\gamma}$ doit être un entier, et ainsi on peut faire $I = \frac{H\delta}{2}$. Ces valeurs étant substituées dans l'équation $DD^{\circ} + I^2 = A$, on aura

$$(4\theta\lambda + H^2)\delta^2 = 4A = g^2 - 4fh.$$

Donc si le nombre $g^2 - 4fh$ n'a point de diviseur quarré, on aura nécessairement $\delta = 1$, et ainsi il sera démontré que $\frac{\zeta}{D}$ est un entier; mais si $g^2 - 4fh$ a un facteur quarré $\delta^2$, l'équation précédente pourra avoir lieu, et il faut examiner les conséquences ultérieures qu'elle fournit.

Or on a $I = \mu D^{\circ} - I^{\circ}$, ou $I^{\circ} = \mu^{\circ} D^{\circ} - I = \mu^{\circ}\lambda\delta - \frac{H\delta}{2}$; donc $I^{\circ}$ est divisible par $\delta$. On a ensuite $D = D^{\circ\circ} + \mu^{\circ}(I^{\circ} - I)$, d'où l'on tire $D^{\circ\circ} = D - \mu^{\circ}(I^{\circ} - I)$. Le second membre étant encore divisible par $\delta$, il faut que le premier $D^{\circ\circ}$ le soit aussi, de même que $I^{\circ\circ}$ dont la valeur est $\mu^{\circ\circ} D^{\circ\circ} - I^{\circ}$. De-là on voit que non-

seulement les trois termes du quotient-complet $\frac{\sqrt{A}+I}{D}$ sont divisibles par $\delta$, mais qu'il en est de même des trois termes des quotiens-complets précédens $\frac{\sqrt{A}+I^{\circ}}{D^{\circ}}$, $\frac{\sqrt{A}+I^{\circ\circ}}{D^{\circ\circ}}$, &c. Remontant ainsi jusqu'à la valeur primitive de $x$, on verra que $\delta$ ne peut être qu'un facteur qui affecte inutilement les trois termes de la quantité $\frac{-\frac{1}{2}g+\sqrt{A}}{f}$; et comme on peut supposer qu'un tel facteur n'existe pas, ou qu'on s'en est débarrassé par la division, on aura donc nécessairement $\delta=1$; et par conséquent $\frac{c}{D}$ ou $\psi$ est toujours un nombre entier.

(57) Lorsque $g$ est pair, le nombre $A$ est entier ainsi que $I$, et alors $\varphi$ ne peut manquer d'être un entier, puisqu'on a $\varphi^2-A\psi^2=\pm1$. Lorsque $g$ est impair, $A$ et $I$ sont des fractions qui ont pour dénominateurs 4 et 2; cependant il peut arriver même dans ce cas, que $\psi$ soit pair, et alors $\varphi$ sera encore un entier, en vertu de l'équation $\varphi^2-A\psi^2=\pm1$.

Enfin, si on a à-la-fois $g$ et $\psi$ impairs, $\varphi$ contiendra la fraction $\frac{1}{2}$; et en faisant $\varphi=\frac{1}{2}\omega$, $\sqrt{A}=\frac{1}{2}\sqrt{a}$, on aura $\varphi+\psi\sqrt{A}=\frac{1}{2}\omega+\frac{1}{2}\psi\sqrt{a}$. Je dis maintenant qu'une puissance quelconque entière de $\frac{1}{2}\omega+\frac{1}{2}\psi\sqrt{a}$ ne peut contenir au plus que la fraction $\frac{1}{2}$. En effet, à cause de $\omega^2-a\psi^2=\pm4$, on a

$$(\tfrac{1}{2}\omega+\tfrac{1}{2}\psi\sqrt{a})^2=\tfrac{1}{2}\omega^2\mp1+\tfrac{1}{2}\omega\psi\sqrt{a}$$
$$(\tfrac{1}{2}\omega+\tfrac{1}{2}\psi\sqrt{a})^3=\frac{\omega^3\mp3\omega}{2}+\frac{\psi(\omega^2\mp1)}{2}\sqrt{a}.$$

D'où l'on voit que la seconde puissance contient la fraction $\frac{1}{2}$ seulement, et que la 3ᵉ ne contient aucune fraction, puisque $\omega$ étant impair, $\frac{\omega^3\mp3\omega}{2}$ et $\frac{\omega^2\mp1}{2}$ doivent se réduire à des entiers. Or l'exposant $n$, quel qu'il soit, sera toujours de l'une des formes $3k$, $3k+1$, $3k+2$; donc puisque la puissance $3k$ ne contient pas de fraction, la puissance $n$ ne pourra contenir au plus que la fraction $\frac{1}{2}$. Cette puissance est d'ailleurs représentée par $\Phi+\Psi\sqrt{A}$ ou $\Phi+\frac{1}{2}\Psi\sqrt{a}$; donc les nombres $2\Phi$ et $\Psi$ seront toujours entiers.

On aura d'ailleurs entre ces entiers la relation $4\Phi^2 - 4A\Psi^2 = \pm 4$.

(58) Revenons à la considération des fractions $\frac{p}{q}, \frac{p1}{q1}, \frac{p2}{q2}$, &c. qui dans les périodes successives répondent à un même quotient-complet $\frac{\sqrt{A}+I}{D}$; si l'on désigne par $\frac{P}{Q}$ l'expression générale de ces fractions $\left(\text{laquelle étoit ci-dessus } \frac{p_n}{q_n}\right)$, il faudra qu'on ait

$$fP^2 + gPQ + hQ^2 = \pm D,$$

le signe + ayant lieu, si la fraction $\frac{P}{Q}$ est de rang impair parmi les fractions convergentes, et le signe — si elle est de rang pair.

Or si on substitue dans le premier membre les valeurs trouvées pour $P$ et $Q$, savoir:

$$P = p\Phi - (\tfrac{1}{2}gp + hq)\Psi$$
$$Q = q\Phi + (\tfrac{1}{2}gq + fp)\Psi,$$

on trouvera

$$fP^2 + gPQ + hQ^2 = (fp^2 + gpq + hq^2)(\Phi^2 - A\Psi^2);$$

de sorte que comme on a déjà $fp^2 + gpq + hq^2 = \pm D$, il faut que $\Phi^2 - A\Psi^2$ se réduise à $\pm 1$, ce qui s'accorde avec ce que nous avons déjà démontré (n°. 55). Cette vérification nous fournit de plus une remarque très-importante, savoir qu'on peut changer le signe de $\Psi$ dans les valeurs de $P$ et $Q$, et que les nouvelles valeurs qui en résultent satisfont également à l'équation $fP^2 + gPQ + hQ^2 = \pm D$; or en examinant ces secondes valeurs

$$P = p\Phi + (\tfrac{1}{2}gp + hq)\Psi$$
$$Q = q\Phi - (\tfrac{1}{2}gq + fp)\Psi,$$

et les comparant aux premières où $\Psi$ a un signe contraire, on trouvera qu'elles ne sont point comprises dans celles-ci, ou du moins qu'elles ne le sont qu'en supposant l'exposant $n$ négatif (c'est ce qu'on développera davantage ci-après). Il faut donc nécessairement que ces nouvelles valeurs de $P$ et $Q$ résultent du développement de l'autre racine de la même équation $fx^2 + gx + h = 0$.

(59) Il suffit, par conséquent, pour résoudre l'équation proposée $fy^2 + gyz + hz^2 = \pm D$, lorsque $D$ n'excède pas $\sqrt{(\tfrac{1}{4}g^2 - fh)}$,

de développer en fraction continue une seule racine de l'équation $fx^2+gx+h=0$, et la solution qu'on obtiendra par le moyen des fractions convergentes qui répondent au quotient-complet $\frac{\sqrt{A}+I}{D}$, comprendra également, par un simple changement de signe, la solution qui naîtroit du développement de l'autre racine. Ces deux solutions seront réunies dans les formules générales

$$y = p\Phi \pm (\tfrac{1}{2}gp+hq)\Psi$$
$$z = q\Phi \mp (\tfrac{1}{2}gq+fp)\Psi;$$

et s'il arrive que le nombre donné $D$ ne se trouve nulle part parmi les dénominateurs des quotiens-complets dans le développement d'une racine, il sera inutile de chercher ce même nombre dans le développement de l'autre racine, et on pourra dès-lors assurer que l'équation dont il s'agit n'est pas résoluble en nombres entiers.

Pour éviter tout embarras à l'égard des signes dans l'application des formules précédentes, faisons $pq^{\circ}-p^{\circ}q=i$, $i$ pouvant être $+1$ ou $-1$ selon les différens cas, on aura d'abord

$$fp^2+gpq+hq^2=iD.$$

Il faudra ensuite faire attention au nombre de termes de la période $\mu$, $\mu'$..... $\omega$ : si ce nombre est pair, les diverses fractions convergentes $\frac{p}{q}$, $\frac{p1}{q1}$, $\frac{p2}{q2}$, &c. seront placées de la même manière, c'est-à-dire qu'elles seront toutes de rang pair, ou toutes de rang impair, et ainsi l'équation $fy^2+gyz+hz^2=iD$ sera résolue par les formules

$$y = p\Phi \pm (\tfrac{1}{2}gp+hq)\Psi$$
$$z = q\Phi \mp (\tfrac{1}{2}gq+fp)\Psi'$$

où l'on a $(\phi+\psi\sqrt{A})^n = \Phi+\Psi\sqrt{A}$.

Dans ce cas, l'équation $fy^2+gyz+hz^2=-iD$ ne pourra être résolue en nombres entiers, au moins d'après la fraction convergente $\frac{p}{q}$.

Si au contraire le nombre des termes de la période est impair, alors on pourra, par les mêmes formules, résoudre à-la-fois l'équation $fy^2+gyz+hz^2=+iD$ et l'équation $fy^2+gyz+hz^2=-iD$,

savoir, la première, en faisant $n=2k$, et la seconde, en faisant $n=2k+1$.

(60) Le cas de $D=1$ devant recevoir un grand nombre d'applications, il sera bon de l'examiner en particulier. On aura alors $\frac{q^{\circ}}{q}+I=\frac{1}{2}g+f\frac{p}{q}$; or $\frac{1}{2}g+f\frac{p}{q}$ est une valeur fort approchée de $\sqrt{A}$ ou de $\frac{1}{2}\sqrt{(g^2-4fh)}$; soit donc, si $g$ est impair, $m$ l'entier impair le plus grand contenu dans $\sqrt{(g^2-4fh)}$, et si $g$ est pair, $m$ l'entier pair le plus grand contenu dans ce même radical, on aura dans les deux cas (parce que $\frac{q^{\circ}}{q}$ est plus petit que l'unité)

$$I=\frac{m}{2}.$$

Le quotient-complet $\frac{\sqrt{A}+I}{D}$ deviendra en même temps $\sqrt{A}+\frac{1}{2}m$, et ainsi l'entier compris $\mu=m$. C'est la valeur du quotient qui dans les périodes successives répond à la valeur $D=1$.

Soit toujours $\mu$, $\mu'$, $\mu''$.... $\omega$, la période des quotiens, et $\frac{\alpha}{\mathcal{C}}$ la fraction qui en résulte, nous avons trouvé ci-dessus $\frac{2\mathcal{C}I}{D}=\alpha-\mathcal{C}^{\circ}$; donc lorsque $D=1$ et $I=\frac{m}{2}$, on a $\mathcal{C}^{\circ}=\alpha-m\mathcal{C}=\alpha-\mu\mathcal{C}$. D'où l'on voit que les quotiens $\mu'$, $\mu''$,... $\omega$ forment une suite symmétrique (n°. 32), et ainsi la période qui se répète à l'infini est de la forme $m$, $\mu'$, $\mu''$,... $\mu''$, $\mu'$. Enfin on aura dans le même cas $\varphi=\alpha-\frac{1}{2}m\mathcal{C}$, $\psi=\mathcal{C}$.

(61) Quel que soit le nombre $D$, si $g$ est pair, les formules générales peuvent être simplifiées et débarrassées de fractions. Soit alors l'équation à résoudre $ay^2+2byz+cz^2=\pm D$, ce qui donnera $f=a$, $g=2b$, $h=c$, $A=bb-ac$; soit toujours $\mu$, $\mu'$, $\mu''$... $\omega$ la période qui répétée une infinité de fois, forme le développement du quotient-complet $\frac{\sqrt{A}+I}{D}$; si par le moyen de cette période, on calcule la fraction $\frac{\alpha}{\mathcal{C}}$ comme il suit:

Quotiens

Quotiens...... $\mu$, $\mu'$, $\mu''$........ $\omega$

Fract. converg. $\frac{1}{0}$, $\frac{\mu}{1}$............ $\frac{\alpha^\circ}{\mathcal{C}^\circ}$, $\frac{\alpha}{\mathcal{C}}$;

on aura $\varphi = \frac{\alpha + \mathcal{C}^\circ}{2} = \alpha - \frac{\mathcal{C}}{D} I$, $\psi = \frac{\mathcal{C}}{D}$, lesquelles valeurs seront toujours des entiers. Faisant ensuite

$$(\varphi + \psi \sqrt{A})^n = \Phi + \Psi \sqrt{A}$$
$$y = p\Phi \pm (bp + cq)\Psi$$
$$z = q\Phi \mp (bq + ap)\Psi,$$

on aura $ay^2 + 2byz + cz^2 = \pm D$, et quant à l'ambiguité du signe, elle sera déterminée par la formule

$$ay^2 + 2byz + cz^2 = (\varphi^2 - A\psi^2)^n (pq^\circ - p^\circ q) D,$$

où l'on sait que $\varphi^2 - A\psi^2$, ainsi que $pq^\circ - p^\circ q$, ne peuvent être que $+1$ ou $-1$.

Les nombres $\varphi$ et $\psi$ trouvés, comme on vient de le dire, par le calcul d'une période, seront toujours les plus simples qui satisfont à l'équation $\varphi^2 - A\psi^2 = \pm 1$; car s'ils ne l'étoient pas, il faudroit supposer, ou que la période dont il s'agit est composée de plusieurs périodes plus courtes, ou qu'il y a des solutions de l'équation proposée non comprises parmi les fractions convergentes. Or le premier cas n'a pas lieu par hypothèse, et le second est impossible, comme il sera prouvé dans le §. XII. Donc les nombres $\Phi$ et $\Psi$ ne dépendent que du seul nombre $A$, et ils se trouveront immédiatement par la Table XII, lorsque $A$ n'excédera pas 1003.

Il est inutile d'ajouter que si le même nombre $D$ se rencontre plusieurs fois dans le cours d'une même période, on pourra produire un pareil nombre de solutions différentes de l'équation proposée.

## §. X. *Comparaison des fractions continues résultantes du développement des deux racines d'une même équation du second degré.*

(62) Nous avons déjà observé (n°. 58) que les deux racines d'une même équation du second degré, $fx^2+gx+h=0$, réduites en fraction continue, concourent également à la résolution de l'équation $fy^2+gyz+hz^2=\pm D$, en sorte que les mêmes valeurs de $D$ doivent se rencontrer nécessairement dans les deux suites de quotiens-complets qui résultent du développement de ces deux racines. Nous allons maintenant mettre cette propriété dans tout son jour, et nous démontrerons d'une manière générale, que si la suite des quotiens-complets, lorsqu'elle est devenue régulière, procède ainsi dans le développement d'une racine :

$$\frac{\sqrt{A}+I^\circ}{D^\circ} = \mu^\circ +$$
$$\frac{\sqrt{A}+I}{D} = \mu +$$
$$\frac{\sqrt{A}+I'}{D'} = \mu' +$$
&c.

le développement de la seconde racine fournira, au moins après l'anomalie des premiers termes, cette autre suite dans l'ordre inverse :

$$\frac{\sqrt{A}+I'}{D} = \mu +$$
$$\frac{\sqrt{A}+I}{D^\circ} = \mu^\circ +$$
$$\frac{\sqrt{A}+I^\circ}{D^{\circ\circ}} = \mu^{\circ\circ} +$$

laquelle retombera nécessairement sur le premier terme $\frac{\sqrt{A}+I'}{D}$, et recommencera ainsi à l'infini.

Considérons de nouveau le développement de la racine $x=\frac{\sqrt{A}-\frac{1}{2}g}{f}$ en fraction continue, et soient $\frac{p^{\circ}}{q^{\circ}}, \frac{p}{q}, \frac{p'}{q'}$ trois fractions convergentes consécutives prises dans la première période des quotiens (1), après que toute irrégularité a cessé, et lorsqu'on s'est assuré que cette même période doit se répéter à l'infini. Nous représenterons à l'ordinaire les trois quotiens-complets correspondans par $\frac{\sqrt{A}+I^{\circ}}{D^{\circ}}$, $\frac{\sqrt{A}+I}{D}$, $\frac{\sqrt{A}+I'}{D'}$, et les entiers qui y sont compris par $\mu^{\circ}, \mu, \mu'$. Quant à la période de quotiens, elle sera $\mu, \mu', \mu'' \ldots \mu^{\circ}$ si on la fait commencer au terme $\mu$; elle seroit également $\mu', \mu'' \ldots \mu^{\circ}, \mu$, si on la faisoit commencer au terme $\mu'$ et ainsi à volonté; en général, la période dont il s'agit peut commencer par tel terme qu'on voudra, mais il faut qu'elle soit composée des mêmes termes, rangés dans le même ordre.

Cela posé, nous avons vu (nº. 54), que si on cherche les diverses fractions convergentes $\frac{p}{q}, \frac{p1}{q1}, \frac{p2}{q2}$, &c. qui dans les périodes successives occupent la même place, ou répondent au même quotient-complet $\frac{\sqrt{A}+I}{D}$, l'expression générale de ces fractions $\frac{p_n}{q_n}$ est donnée par les formules

$$p_n = p\Phi - (\tfrac{1}{2}gp + hq)\Psi$$
$$q_n = q\Phi + (\tfrac{1}{2}gq + fp)\Psi, \qquad (a)$$

où l'on a

$\Phi+\Psi\sqrt{A}=(\varphi+\psi\sqrt{A})^n$, et $\Phi^2-A\Psi^2=(\varphi^2-A\psi^2)^n=(\pm 1)^n$.

Il suffit donc de donner à $n$ les valeurs successives 0, 1, 2, 3, &c., et de substituer les valeurs de $\Phi$ et $\Psi$ qui en résultent, pour avoir successivement toutes les fractions convergentes dont il s'agit $\frac{p}{q}, \frac{p1}{q1}, \frac{p2}{q2}$, &c. Il reste à voir maintenant ce qui arriveroit, si on donnoit à $n$ des valeurs négatives $-1$, $-2$, $-3$, &c.

(1) Cette période pourroit contenir moins de trois termes, mais alors on réuniroit plusieurs périodes, afin de ne pas donner lieu à exception pour ce cas particulier.

(63) Or j'observe qu'on a

$$(\varphi+\psi\sqrt{A})^{-n}=(\varphi^2-A\psi^2)^{-n}\,(\varphi-\psi\sqrt{A})^n=(\pm 1)^n\,(\Phi-\Psi\sqrt{A});$$

donc la supposition de $n$ négatif revient simplement à changer $\Psi$ de signe, et à multiplier les valeurs de $\Phi$ et $\Psi$ par un même facteur $(\pm 1)^n$, cette quantité ambigue $\pm 1$ venant de $\varphi^2-A\psi^2$ qui en effet peut être $+1$, ou $-1$. Mais comme la fraction $\frac{p_n}{q_n}$ n'est pas différente de $\frac{-p_n}{-q_n}$, on peut faire abstraction du facteur $(\pm 1)^n$, et ainsi les valeurs négatives de $n$ répondront à de nouvelles valeurs de $\frac{p_n}{q_n}$ données par les formules

$$p_n=p\Phi+(\tfrac{1}{2}gp+hq)\Psi$$
$$q_n=q\Phi-(\tfrac{1}{2}gq+fp)\Psi. \qquad (b)$$

On pourroit croire d'abord que ces formules ne diffèrent des premières que par la forme, et qu'elles conduisent réellement aux mêmes valeurs de $\frac{p_n}{q_n}$; mais il faudroit pour cela que deux fractions telles que

$$\frac{p\Phi-(\tfrac{1}{2}gp+hq)\Psi}{q\Phi+(\tfrac{1}{2}gq+fp)\Psi},\quad \frac{p\Phi'+(\tfrac{1}{2}gp+hq)\Psi'}{q\Phi'-(\tfrac{1}{2}gq+fp)\Psi'}$$

pussent être égales : or c'est ce qui ne peut jamais avoir lieu, car en les réduisant au même dénominateur, on trouve que la différence des numérateurs est $(fp^2+gpq+hq^2)\,(\Phi'\Psi+\Phi\Psi')$, quantité qui ne peut jamais être nulle.

Donc il est certain que les formules ($b$) donnent des valeurs de $\frac{p_n}{q_n}$ différentes de celles que donnent les formules ($a$). Mais en faisant, soit dans les formules ($b$), soit dans les formules ($a$), $p_n=y$, $q_n=z$, les valeurs générales de $y$ et de $z$ satisfont à l'équation $fy^2+gyz+hz^2=\pm D$; d'un autre côté, $D$ étant supposé plus petit que $\sqrt{A}$, on peut démontrer que toute fraction $\frac{y}{z}$ qui satisfait à cette équation est comprise parmi les fractions convergentes vers une racine de l'équation $fx^2+gx+h=0$. Donc si les formules ($b$) donnent des fractions $\frac{p_n}{q_n}$ non comprises parmi

les fractions convergentes vers la racine $x = \frac{\sqrt{A} - \frac{1}{2}g}{f}$; il faut que ces mêmes fractions $\frac{p_n}{q_n}$ soient comprises parmi les fractions convergentes vers l'autre racine $x' = \frac{-\sqrt{A} - \frac{1}{2}g}{f}$.

On ne doit pas perdre de vue, que parmi les fractions convergentes qui répondent au quotient-complet $\frac{\sqrt{A} + I}{D}$, $\frac{p}{q}$ est supposée la plus simple, ou celle qui est comprise dans la première période. Si on fait $n = -1$ dans les formules $(a)$, ou $n = 1$ dans les formules $(b)$, la fraction qui en résulte pourra tomber dans les parties irrégulières du développement de l'une ou de l'autre racine, ou même ne se trouver dans aucune, par des raisons qui seront exposées ailleurs; mais si on fait $n > 1$ dans les formules $(b)$, alors la fraction qui en résultera sera certainement l'une des fractions convergentes vers la racine $x = \frac{-\sqrt{A} - \frac{1}{2}g}{f}$.

(64) Soit donc, en supposant $n > 1$, $(\varphi + \psi\sqrt{A})^n = \Phi + \Psi\sqrt{A}$, et

$$P = p\Phi + (\tfrac{1}{2}gp + hq)\Psi$$
$$Q = q\Phi - (\tfrac{1}{2}gq + fp)\Psi,$$

on aura $\frac{P}{Q}$ pour l'une des fractions convergentes vers la racine $x' = \frac{-\sqrt{A} - \frac{1}{2}g}{f}$. Mais si on fait semblablement

$$P^\circ = -p'\Phi - (\tfrac{1}{2}gp' + hq')\Psi$$
$$Q^\circ = -q'\Phi + (\tfrac{1}{2}gq' + fp')\Psi$$

$$P' = -p^\circ\Phi - (\tfrac{1}{2}gp^\circ + hq^\circ)\Psi$$
$$Q' = -q^\circ\Phi + (\tfrac{1}{2}gq^\circ + fp^\circ)\Psi,$$

il est clair que $\frac{P^\circ}{Q^\circ}$ et $\frac{P'}{Q'}$ seront pareillement des fractions convergentes vers la même racine. Il s'agit maintenant de faire voir que les trois fractions convergentes $\frac{P^\circ}{Q^\circ}$, $\frac{P}{Q}$, $\frac{P'}{Q'}$, se suivent immédiatement dans l'ordre où elles sont écrites.

Et d'abord les valeurs précédentes donnent $PQ^\circ - P^\circ Q = (p'q - pq')(\Phi^2 - A\Psi^2) = \pm 1$, et $(P'Q - PQ') = -(PQ^\circ - P^\circ Q)$; conditions toutes deux nécessaires pour l'objet que nous avons en vue, mais elles ne sont pas encore suffisantes.

On peut, pour fixer les idées, supposer que la valeur de $n$ est un peu grande, en sorte que la fraction convergente $\frac{P}{Q}$ réponde à une période assez éloignée du commencement de la suite. Comme toutes les périodes sont égales, il importe peu quelle est celle qu'on considère; et la forme qu'on trouvera pour une période éloignée, conviendra également à toutes les autres périodes. Or lorsque $n$ est un peu grand, les nombres $\Phi$ et $\Psi$ sont très-considérables, et comme on a toujours $\Phi^2 - A\Psi^2 = (\pm 1)^n = \pm 1$, il s'ensuit qu'on a alors à très-peu-près $\Phi = \Psi\sqrt{A}$; substituant cette valeur dans celle de $P$, on aura $P = \Psi(p\sqrt{A} + \frac{1}{2}gp + hq) = \Psi(\sqrt{A} + \frac{1}{2}g)(p - qx)$, $x$ désignant la première racine $\frac{\sqrt{A} - \frac{1}{2}g}{f}$ dont $\frac{p}{q}$ est une valeur approchée.

On trouvera de semblables valeurs pour $P^\circ$ et $P'$, et si pour abréger on appelle $R$ le facteur constant $\Psi(\sqrt{A} + \frac{1}{2}g)$, on aura

$$P^\circ = -R(p' - q'x)$$
$$P = R(p - qx)$$
$$P' = -R(p^\circ - q^\circ x).$$

Soit $z$ le quotient-complet qui répond à la fraction convergente $\frac{p}{q}$ dans le développement de la valeur de $x$, on aura $x = \frac{pz + p^\circ}{qz + q^\circ}$, ou $z = \frac{-(p^\circ - q^\circ x)}{p - qx}$; or $z$ doit être positif et plus grand que l'unité; donc $-(p^\circ - q^\circ x)$ est plus grand que $p - qx$ et de même signe; par la même raison, $(p - qx)$ est de même signe, et plus grand que $-(p' - q'x)$; donc les trois nombres $P^\circ, P, P'$ sont de même signe, et ils se suivent par ordre de grandeur, en sorte qu'on a $P^\circ < P$, $P < P'$. On démontreroit la même chose des trois nombres $Q^\circ$, $Q$, $Q'$; et cela posé, si les deux fractions convergentes

$\frac{P^\circ}{Q^\circ}$, $\frac{P}{Q}$, ne se suivent pas immédiatement, on ne peut du moins concevoir d'intermédiaire entr'elles que la fraction $\frac{P-P^\circ}{Q-Q^\circ}$; car comme on a déjà $PQ^\circ - P^\circ Q = \pm 1$, et qu'en représentant par $\frac{M}{N}$ la fraction convergente qui précède $\frac{P}{Q}$, on doit avoir aussi $PN - MQ = \pm 1$, il s'ensuit qu'on a $M = kP \pm P^\circ$, et $N = kQ \pm Q^\circ$, $k$ étant un nombre indéterminé. Or la condition que $M$ soit comprise entre $P$ et $P^\circ$, donne $k = 1$, $M = P - P^\circ$, $N = Q - Q^\circ$. Ainsi on est assuré que la fraction convergente $\frac{P}{Q}$ est précédée de $\frac{P^\circ}{Q^\circ}$, ou qu'au moins elle l'est de $\frac{P-P^\circ}{Q-Q^\circ}$.

(65) L'incertitude à cet égard va bientôt être fixée, en déterminant le quotient-complet qui répond à la fraction $\frac{P}{Q}$. Soit $z$ ce quotient-complet dans l'hypothèse que $\frac{P^\circ}{Q^\circ}$ précède $\frac{P}{Q}$, alors la valeur entière de la fraction continue seroit $\frac{Pz + P^\circ}{Qz + Q^\circ}$; soit $y$ le quotient-complet dans l'hypothèse que $\frac{P-P^\circ}{Q-Q^\circ}$ précède $\frac{P}{Q}$, on auroit la valeur de la fraction continue

$$= \frac{Py + P - P^\circ}{Qy + Q - Q^\circ} = \frac{-P(y+1) + P^\circ}{-Q(y+1) + Q^\circ}.$$

Or il est clair que cette seconde hypothèse est renfermée dans la première, en supposant $z = -y - 1$; donc si en partant de la première hypothèse, on trouve une valeur positive de $z$, ce sera une preuve que cette hypothèse est légitime, et qu'en effet $\frac{P^\circ}{Q^\circ}$, $\frac{P}{Q}$ sont des fractions convergentes consécutives. Si au contraire le calcul donne pour $z$ une valeur négative, on en conclura que la seconde hypothèse est la véritable.

Or je dis que la valeur de $z$ est non-seulement positive, mais qu'elle est en général $\frac{\sqrt{A} + I'}{D}$; je dis de plus que l'entier com-

pris dans cette quantité est $\mu$. Si ce dernier point est vrai, il faudra donc qu'on ait $P' = \mu P + P^\circ$, $Q' = \mu Q + Q^\circ$, et c'est en effet ce qui se vérifie immédiatement par les valeurs de $P$, $Q$, $P^\circ$, $Q^\circ$, &c., puisqu'on a toujours $p' = \mu p + p^\circ$, et $q' = \mu q + q^\circ$. Au reste, la seconde partie peut se prouver généralement ainsi.

On a d'abord $I' = \mu D - I$, ce qui donne $\frac{\sqrt{A} + I'}{D} = \mu + \frac{\sqrt{A} - I}{D}$;

d'ailleurs la valeur de $q^\circ$ trouvée n°. 54, donne $\frac{q^\circ}{q} = \frac{\frac{1}{2}g - I}{D} + \frac{f}{D} \cdot \frac{p}{q}$;

et comme $\frac{p}{q}$ est déjà une valeur fort approchée de $\frac{\sqrt{A} - \frac{1}{2}g}{f}$, on a à très-peu-près $\frac{q^\circ}{q} = \frac{\frac{1}{2}g - I}{D} + \frac{f}{D} \cdot \frac{\sqrt{A} - \frac{1}{2}g}{f} = \frac{\sqrt{A} - I}{D}$; d'où l'on voit que $\frac{\sqrt{A} - I}{D}$, égale à très-peu-près à $\frac{q^\circ}{q}$, est toujours plus petite que l'unité, et ainsi on a, suivant la notation accoutumée, $\frac{\sqrt{A} + I'}{D} = \mu +$.

Venons à la première partie de notre assertion. Si $\frac{\sqrt{A} + I'}{D}$ est le quotient-complet qui répond à la fraction convergente $\frac{P}{Q}$, et que celle-ci soit précédée de $\frac{P^\circ}{Q^\circ}$, il faudra donc que la seconde racine $x'$ de l'équation $fx^2 + gx + h = 0$, ait pour valeur

$$x' = \frac{P(\sqrt{A} + I') + P^\circ D}{Q(\sqrt{A} + I') + Q^\circ D}.$$

Mettant au lieu de $I'$ sa valeur $\mu D - I$, et observant qu'on a $\mu P + P^\circ = P'$, $\mu Q + Q^\circ = Q'$, cette équation deviendra

$$x' = \frac{P(\sqrt{A} - I) + P' D}{Q(\sqrt{A} - I) + Q' D}.$$

Si on y substitue ensuite les valeurs de $P$, $Q$, $P'$, $Q'$, et que dans le résultat on mette au lieu de $p^\circ$ et $q^\circ$ leurs valeurs trouvées n°. 54, on aura

$$x' = \frac{\phi(p\sqrt{A} + \frac{1}{2}gp + hq) + \psi(\frac{1}{2}gp\sqrt{A} + hq\sqrt{A} + Ap)}{\phi(q\sqrt{A} - \frac{1}{2}gq - fp) - \psi(\frac{1}{2}gq\sqrt{A} + fp\sqrt{A} - Aq)},$$

quantité

quantité qu'on peut mettre sous la forme

$$x' = \frac{(\Phi+\Psi\sqrt{A})\ (p\sqrt{A}+\tfrac{1}{2}gp+hq)}{(\Phi+\Psi\sqrt{A})\ (q\sqrt{A}-\tfrac{1}{2}gq-fp)};$$

de sorte qu'en supprimant le facteur commun aux deux termes, on aura

$$x' = \frac{p\sqrt{A}+\tfrac{1}{2}gp+hq}{q\sqrt{A}-\tfrac{1}{2}gq-fp}.$$

Mais à cause de $A=\tfrac{1}{4}g^2-fh$, on a $h=\dfrac{(\tfrac{1}{2}g+\sqrt{A})\ (\tfrac{1}{2}g-\sqrt{A})}{f}$,

et ainsi $p\sqrt{A}+\tfrac{1}{2}gp+hq=\dfrac{(\sqrt{A}+\tfrac{1}{2}g)}{f}(fp+\tfrac{1}{2}gq-q\sqrt{A})$; donc enfin la valeur de $x'$ se réduit à

$$x' = \frac{-\sqrt{A}-\tfrac{1}{2}g}{f};$$

ce qui est la seconde racine de l'équation $fx^2+gx+h=0$.

(66) Ce résultat justifie pleinement les diverses propositions que nous avons avancées, et il en résulte, pour principale conséquence, que $\dfrac{\sqrt{A}+I'}{D}$ est le quotient-complet qui dans le développement de la seconde racine $x'$, répond à la fraction convergente $\dfrac{P}{Q}$. Par la même raison, le quotient-complet qui répond à la fraction suivante $\dfrac{P'}{Q'}$, est $\dfrac{\sqrt{A}+I}{D^{\circ}}$, celui qui vient immédiatement après est $\dfrac{\sqrt{A}+I^{\circ}}{D^{\circ\circ}}$, &c.; d'où l'on voit que les dénominateurs $D$, $D^{\circ}$, $D^{\circ\circ}$, &c. suivent un ordre contraire à celui qu'ils ont dans le développement de la première racine.

Au reste l'existence du quotient-complet $\dfrac{\sqrt{A}+I'}{D}$ suffit pour prouver celle des quotiens-complets suivans, qu'on en déduit par l'opération ordinaire du développement en fraction continue. En effet, on a déjà vu que l'entier compris dans $\dfrac{\sqrt{A}+I'}{D}$ est $\mu$;

de-là, et des relations déjà connues par le développement de la première racine, on tire la suite

$$\frac{\sqrt{A}+I'}{D}=\mu+\frac{\sqrt{A}-I}{D}$$

$$\frac{D}{\sqrt{A}-I}=\frac{\sqrt{A}+I}{D^{\circ}}=\mu^{\circ}+\frac{\sqrt{A}-I^{\circ}}{D^{\circ}}$$

$$\frac{D^{\circ}}{\sqrt{A}-I^{\circ}}=\frac{\sqrt{A}+I^{\circ}}{D^{\circ\circ}}=\mu^{\circ\circ}+\frac{\sqrt{A}-I^{\circ\circ}}{D^{\circ\circ}}$$

&c.

Mais la suite des quotiens $\mu$, $\mu^{\circ}$, $\mu^{\circ\circ}$, &c. retombera nécessairement sur le quotient $\mu$; et ainsi la période qui règne dans le développement de la seconde racine, est composée des mêmes termes que la période de la première racine, avec cette seule différence que les termes y sont rangés dans un ordre inverse.

S'il arrivoit que la période qui règne dans le développement d'une racine fût de la forme $\mu$, $\mu'$, $\mu''\ldots\mu''$, $\mu'$, $\mu$, $k$, c'est-à-dire fût composée d'une partie symmétrique, précédée ou suivie d'un terme isolé $k$, alors le renversement donneroit toujours la même période, laquelle par conséquent seroit commune aux deux racines de l'équation. C'est ce qui s'observe dans un grand nombre de cas, et alors les mêmes quotiens-complets se trouvent aussi dans le développement des deux racines, et y suivent le même ordre.

## §. XI. Résolution en nombres entiers de l'équation $Ly^2 + Myz + Nz^2 = \pm H$.

(67) Il faut distinguer deux cas, selon que $y$ et $z$ sont ou ne sont pas premiers entr'eux. Pour ramener le second cas au premier, soit $\theta$ la plus grande commune mesure de $y$ et de $z$, et soit $y = \theta y'$, $z = \theta z'$, alors le premier membre étant divisible par $\theta^2$, il faudra que $H$ soit aussi divisible par $\theta^2$. Soit donc $H = \theta^2 H'$, on aura

$$Ly'^2 + My'z' + Nz'^2 = \pm H',$$

équation dans laquelle $y'$ et $z'$ sont maintenant premiers entr'eux. Donc autant il y aura de quarrés $\theta^2$ qui peuvent diviser $H$, autant on aura à résoudre d'équations semblables à la précédente dans lesquelles les indéterminées seront des nombres premiers entr'eux.

On peut supposer que cette sorte de décomposition a été faite par une opération préliminaire, et ainsi nous regarderons l'équation proposée $Ly^2 + Myz + Nz^2 = \pm H$ comme l'une de celles où il faut que les indéterminées $y$ et $z$ soient des nombres premiers entr'eux.

Cela posé, nous distinguerons encore le cas où $z$ et $H$ sont premiers entr'eux, et celui où ils ont un commun diviseur $\theta$. Dans ce dernier cas, soit $z = \theta z'$, $H = \theta H'$, il faudra que $\frac{Ly^2}{\theta}$ soit un entier; mais comme $y$ n'a aucun diviseur commun avec $z$, ni par conséquent avec $\theta$, cette condition exige que $L$ soit divisible par $\theta$. Soit donc $L = \theta L'$, et l'équation à résoudre deviendra

$$L'y^2 + Myz' + Nz'^2 = \pm H',$$

dans laquelle maintenant on peut considérer $z'$ et $H'$ comme premiers entr'eux.

Donc autant il y aura de diviseurs communs entre $L$ et $H$ (l'unité comprise), autant il y aura d'équations à résoudre dans lesquelles $z'$ et $H'$ seront premiers entr'eux. On peut supposer de nouveau que l'équation proposée est ramenée à cet état, ou qu'elle

N 2

est une de celles dans lesquelles l'équation primitive a été décomposée. Ainsi toute la difficulté se réduit à résoudre une ou plusieurs équations, telles que

$$Ly^2+Myz+Nz^2=\pm H',$$

dans laquelle $z$ et $y$ sont premiers entr'eux, ainsi que $z$ et $H$. Or cette équation présente différens cas à examiner, selon que le nombre $4LN-M^2$ est positif, zéro ou négatif; c'est-à-dire, selon que les deux facteurs du premier membre sont imaginaires, égaux ou réels.

(68) Soit d'abord $4LN-M^2=$ à un nombre positif $B$; si on multiplie l'équation proposée par $4L$, et qu'on fasse $2Ly+Mz=x$, on aura

$$x^2+Bz^2=+4LH$$

(nous mettons + seulement dans le second membre, parce qu'on voit bien que le signe — ne pourroit avoir lieu). Or ayant à résoudre l'équation $x^2+Bz^2=C$, la méthode la plus simple est de calculer successivement les différentes valeurs de la quantité $C-Bz^2$, en faisant $z=0, 1, 2, 3...$ jusqu'à $z=\sqrt{\frac{C}{B}}$. Si parmi ces valeurs il se trouve un quarré, et qu'en même temps la racine $x$ de ce quarré rende $\frac{Mz\pm x}{2L}$ égal à un entier, on aura une solution de l'équation proposée. Mais si ces deux conditions ne peuvent être remplies à-la-fois, on en conclura que l'équation proposée n'est pas résoluble en nombres entiers.

Il est évident que dans ce premier cas il ne pourra jamais y avoir qu'un nombre limité de solutions en nombres entiers. Ce cas d'ailleurs est si simple, qu'il n'exige aucune des préparations indiquées dans l'article précédent, et qu'on peut procéder à la résolution, comme il vient d'être dit, sans s'embarrasser si $y$, $z$ et $H$ ont ou n'ont pas de commun diviseur.

(69) Prenons pour exemple l'équation $15y^2+43yz+32z^2=223$: si on multiplie les deux membres par 60, et qu'on fasse $30y+43z=x$, la transformée sera

$$x^2+71z^2=13380.$$

Je calcule donc les valeurs de la quantité $13380 - 71z^2$, en faisant successivement $z = 0, 1, 2, 3$, &c., jusqu'à ce que la quantité dont il s'agit cesse d'être positive ; les résultats qu'on obtient facilement, au moyen de leurs différences uniformément croissantes, sont :

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Valeurs de $x^2$... | 13380, | 13309, | 13096, | 12741, | 12244, | 11605, | 10824, |
| Différences .... | 71, | 213, | 355, | 497, | 639, | 781, | 923, |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Valeurs de $x^2$... | 9901, | 8836, | 7629, | 6280, | 4789, | 3156, | 1381. |
| Différences .... | 1065, | 1207, | 1349, | 1491, | 1633, | 1775. | |

Or parmi ces résultats, il n'y a que 8836 qui soit un quarré parfait, celui de 94, ainsi les seules valeurs de $z$ et $x$ à employer sont $z = 8$ et $x = \pm 94$ ; mais de-là résulte $y = \frac{\pm 94 - 344}{30}$ et cette valeur ne se réduit pas à un nombre entier ; ainsi l'équation proposée n'est pas résoluble en nombres entiers ; on peut seulement y satisfaire par des valeurs rationnelles telles que $z = 8$, $y = -\frac{25}{3}$, et une infinité d'autres.

(70) Si on a $4LN - M^2 = 0$, ou si les facteurs du premier membre de l'équation proposée sont égaux, il faudra, pour que cette équation soit résoluble, qu'elle soit de la forme $(my + nz)^2 = h^2$, et alors elle se réduit à l'équation du premier degré $my + nz = \pm h$, laquelle sera toujours possible, si $m$ et $n$ sont premiers entr'eux.

Il ne reste donc plus à examiner que le cas où $4LN - M^2$ est égal à un nombre négatif $-B$. Et d'abord si le nombre $B$ est un quarré parfait, les facteurs de la quantité $Ly^2 + Myz + Nz^2$ seront rationnels, et l'équation à résoudre sera de la forme

$$(my + nz)(fy + gz) = \pm H.$$

Or il est visible, que la résolution de cette équation se réduit à celle des deux équations déterminées

$$my + nz = \theta$$
$$fy + gz = \pm \frac{H}{\theta},$$

$\theta$ étant un facteur quelconque de $H$. On prendra donc successi-

vement pour $\theta$ tous les diviseurs de $H$, en y comprenant l'unité, et on résoudra relativement à chacun d'eux, les équations déterminées qui précèdent. On pourra obtenir, par ce moyen, plusieurs solutions, si toutefois les valeurs de $y$ et $z$ qui en résultent sont des entiers; mais dans aucun cas, le nombre de ces solutions ne pourra excéder celui des diviseurs du nombre $H$.

(71) Supposons enfin qu'on ait $M^2-4LN=B$, $B$ n'étant point un quarré parfait. Alors l'équation proposée

$$Ly^2+Myz+Nz^2=\pm H$$

présentera deux cas à examiner, selon que $H$ est $<\frac{1}{2}\sqrt{B}$ ou $>\frac{1}{2}\sqrt{B}$.

Soit I°. $H<\frac{1}{2}\sqrt{B}$; dans ce cas, il suffit de développer en fraction continue une racine de l'équation

$$Lx^2+Mx+N=0;$$

et si parmi les quotiens-complets $\frac{\sqrt{A}+I}{D}$ qui résultent de cette opération, on en trouve un dont le dénominateur $D=H$, on en conclura que l'une au moins des deux équations

$$Ly^2+Myz+Nz^2=+H$$
$$Ly^2+Myz+Nz^2=-H$$

est résoluble, ou même toutes les deux, lorsque les conditions nécessaires sont remplies. Nous avons donné ces conditions dans le paragraphe IX, ainsi que les formules qui contiennent les valeurs complettes de $y$ et $z$, et nous avons remarqué que ces formules renferment le résultat du développement des deux racines de l'équation $Lx^2+Mx+N=0$, de sorte qu'il suffit d'en développer une.

Le nombre $H$ peut se trouver plusieurs fois parmi les valeurs de $D$ dans le cours d'une même période, et il en résulte alors autant de solutions différentes de l'équation proposée. Mais s'il ne se trouve nulle part parmi ces valeurs, on en conclura avec certitude, que l'équation proposée n'est résoluble ni avec le second membre $+H$, ni avec le second membre $-H$.

Ce premier cas de $H<\frac{1}{2}\sqrt{B}$ se résout donc immédiatement, et

avec beaucoup de facilité par le seul développement d'une racine de l'équation $Lx^2+Mx+N=0$ en fraction continue. Il faut même observer que cette solution suppose seulement $y$ et $z$ premiers entr'eux (car $\frac{y}{z}$ étant assimilé à une fraction convergente $\frac{p}{q}$, doit toujours être une fraction irréductible, puisqu'on a $pq^{\circ}-p^{\circ}q=\pm 1$), et ainsi elle n'exige pas que $z$ et $H$ soient premiers entr'eux. On peut donc, par ce moyen, se dispenser de faire la décomposition relative aux facteurs communs de $L$ et de $H$, dont on a fait mention n°. 67, et on aura, par une seule opération, la résolution de toutes les équations de cette sorte. Mais il faut, comme nous l'avons supposé, que $H$ soit $<\frac{1}{2}\sqrt{B}$; de plus, si $H$ contient un facteur quarré $\theta^2$, il faudra, comme nous l'avons déjà indiqué, faire $y=\theta y'$, $z=\theta z'$, $H=\theta^2 H'$, et résoudre, par la même voie, chaque équation $Ly'^2+My'z'+Nz'^2=\pm H'$ pour chaque facteur quarré $\theta^2$ qui peut diviser $H$.

(72) Soit en second lieu $H>\frac{1}{2}\sqrt{B}$, alors on supposera que l'équation est préparée, comme on l'a dit n°. 67, de manière que $y$ et $z$ soient premiers entr'eux, ainsi que $z$ et $H$. On pourra faire alors

$$y=nz+Hu,$$

et ajouter même la condition que $n$ ne surpasse pas $\frac{1}{2}H$; car l'équation précédente subsisteroit en mettant $n-\alpha H$ à la place de $n$, et $u+\alpha z$ à la place de $u$; or il est clair qu'on peut prendre $\alpha$, de manière que $n-\alpha H$ soit compris entre $+\frac{1}{2}H$ et $-\frac{1}{2}H$. Substituant donc la valeur de $y$ dans l'équation proposée, et divisant le résultat par $H$, on aura

$$\left(\frac{Ln^2+Mn+N}{H}\right)z^2+(2nL+M)zu+LHu^2=\pm 1;$$

et puisque $z$ et $H$ sont premiers entr'eux, cette équation ne peut avoir lieu, à moins que $\frac{Ln^2+Mn+N}{H}$ ne soit un entier. On donnera donc à $n$ toutes les valeurs en nombres entiers depuis $-\frac{1}{2}H$ jusqu'à $+\frac{1}{2}H$; et s'il n'en est aucune qui rende la quantité $Ln^2+Mn+N$ divisible par $H$, on prononcera avec certitude que

l'équation proposée n'est pas résoluble. Si au contraire on trouve une ou plusieurs valeurs de $n$ qui remplissent cette condition, il faudra prendre successivement ces différentes valeurs, et faire un calcul séparé pour chacune, comme si l'équation proposée étoit transformée en autant d'équations différentes.

Soit pour abréger $Ln^2+Mn+N=fH$, $2nL+M=g$, $LH=h$, l'équation à résoudre pour chaque valeur de $n$ sera

$$fz^2+gzu+hu^2=\pm 1,$$

où il est à remarquer qu'on a toujours $g^2-4fh=M^2-4LN=B$.

Nous avons donné dans le paragraphe IX une méthode pour résoudre cette équation lorsqu'elle est possible, et les mêmes remarques que nous avons faites lorsque $D$ est $<\frac{1}{2}\sqrt{B}$, sont également applicables dans le cas présent où $D=1$ : ainsi nous n'avons rien à ajouter sur cet objet, d'autant qu'on voit bien qu'ayant trouvé les valeurs générales de $z$ et $u$, on en tire immédiatement celles des indéterminées de l'équation proposée, exprimées pareillement en nombres entiers.

### EXEMPLE I.

(73) Soit proposé de résoudre en nombres entiers l'équation $2x^2-23y^2=105$.

Cette équation se rapporte au cas précédent ; elle n'est point susceptible de se décomposer en plusieurs autres, parce que 105 n'a point de diviseur quarré, ni de commun diviseur avec le coefficient 2. On fera donc $x=ny-105z$, et on déterminera $n<\frac{105}{2}$ de manière que $\dfrac{2n^2-23}{105}$ soit un entier. Plusieurs moyens seront donnés ci-après pour faciliter de semblables recherches ; observons quant à présent, que comme 105 est le produit des nombres premiers 3, 5, 7, il faut chercher séparément trois valeurs de $n$ telles que $\dfrac{2n^2-23}{3}$, $\dfrac{2n^2-23}{5}$, $\dfrac{2n^2-23}{7}$ soient des entiers. Ces valeurs sont respectivement $n=3\alpha\pm1$, $n=5\beta\pm2$, $n=7\gamma\pm1$, les nombres $\alpha$, $\beta$, $\gamma$ étant à volonté. Or ces formules sont faciles à concilier entr'elles, et comme il suffit de considérer les valeurs de

de $n$ positives et moindres que $\frac{105}{2}$, la dernière formule donnera $n = 6, 8, 13, 15, 20, 22, 27, 29, 34, 36, 41, 43, 48, 50$. De-là il faut écarter tous les nombres qui ne satisfont pas à la seconde formule, ou qui divisés par 5 ne laissent pas $\pm 2$ de reste; ainsi les 14 valeurs précédentes se réduisent à celles-ci $n = 8, 13, 22, 27, 43, 48$. Enfin pour satisfaire à la première formule, il faut encore supprimer tous les nombres divisibles par 3, ce qui ne laissera subsister que ces quatre valeurs $n = 8, 13, 22, 43$.

Soit donc 1°. $n = 8$, et $x = 8y - 105z$, la transformée sera

$$y^2 - 32yz + 210z^2 = 1.$$

Toutes les fois qu'on parvient ainsi à une équation de la forme

$$y^2 - 2fyz + gz^2 = +1,$$

on est assuré que la solution est toujours possible, parce qu'en faisant $y - fz = u$, l'équation devient $u^2 - Az^2 = 1$, qui est toujours résoluble. Dans le cas présent, on trouvera par les formules du n°. 61,

$$y = \Phi \pm 16\Psi$$
$$z = \pm \Psi$$
$$(24335 + 3588\sqrt{46})^n = \Phi + \Psi\sqrt{46};$$

d'où résulte pour première solution de la proposée

$$x = 8\Phi \pm 23\Psi$$
$$y = \Phi \pm 16\Psi.$$

(74) Soit 2°. $n = 13$ et $x = 13y - 105z$, la transformée sera

$$3y^2 - 52yz + 210z^2 = 1.$$

Pour résoudre celle-ci, il faut développer en fraction continue une racine de l'équation $3x^2 - 52x + 210 = 0$. Voici l'opération avec le calcul des fractions convergentes prolongé seulement jusqu'à ce qu'on trouve $D = 1$:

| | |
|---|---|
| $x = \frac{\sqrt{46}+26}{3} = 10 +$ | 1 : 0 |
| $\frac{\sqrt{46}+4}{10} = 1 +$ | 10 : 1 |
| $\frac{\sqrt{46}+6}{1} = 12 +$ | 11 : 1 |
| &c. | &c. |

Cela posé, les nombres à substituer dans les formules du n°. 61 sont $p=11$, $q=1$, $a=3$, $b=-26$, $c=210$, $A=46$; d'ailleurs on a déjà trouvé dans le premier cas, que les moindres nombres qui satisfont à l'équation $\varphi^2-46\psi^2=\pm 1$ sont $\varphi=24335$, $\psi=3588$, lesquels donnent $\varphi^2-46\psi^2=+1$; et comme on a en même temps $pq^\circ-p^\circ q=+1$, l'équation proposée $3y^2-52yz+210z^2=+1$ sera résoluble (elle ne le seroit pas si le second membre étoit $-1$); faisant donc toujours

$$(24335+3588\sqrt{46})^x=\Phi+\Psi\sqrt{46},$$

on aura par les substitutions $y=11\Phi\pm 76\Psi$, $z=\Phi\pm 7\Psi$; d'où résulte pour seconde solution

$$x=38\Phi\pm 253\Psi$$
$$y=11\Phi\pm\ \ 76\Psi.$$

*Remarquez* qu'on auroit pu trouver immédiatement les valeurs de $y$ et de $z$ par l'opération seule du développement en fraction continue; car si à la place du quotient-complet $\frac{\sqrt{46}+6}{1}$ qui répond à la fraction convergente $\frac{11}{1}$, on met sa valeur approchée $\frac{\Phi}{\Psi}+6$; et si ensuite, au moyen de ce quotient, considéré comme entier, on calcule la fraction convergente qui suivroit $\frac{11}{1}$, on trouve que cette fraction est $\frac{11\left(6+\frac{\Phi}{\Psi}\right)+10}{1\left(6+\frac{\Phi}{\Psi}\right)+1}$, laquelle se réduit à $\frac{11\Phi+76\Psi}{\Phi+7\Psi}$. C'est la valeur générale de $\frac{y}{z}$ dans laquelle il ne reste plus qu'à donner à $\Psi$ le double signe $\pm$. Il seroit facile de démontrer que ce procédé, qui dispense de recourir aux formules générales, s'accorde entièrement avec elles, et peut par conséquent leur être substitué, même pour une valeur quelconque de $D$.

(75) Soit 3°. $n=22$, et $x=22y-105z$, la transformée sera

$$9yy-88yz+210z^2=1.$$

On développera donc une racine de l'équation $9x^2-88x+210=0$, jusqu'à ce qu'on trouve un quotient-complet dont le dénominateur

soit 1, et on calculera à mesure les fractions convergentes comme il suit :

$$x = \frac{\sqrt{46}+44}{9} = 5 + \qquad 1 : 0$$

$$\frac{\sqrt{46}+1}{5} = 1 + \qquad 5 : 1$$

$$\frac{\sqrt{46}+4}{6} = 1 + \qquad 6 : 1$$

$$\frac{\sqrt{46}+2}{7} = 1 + \qquad 11 : 2$$

$$\frac{\sqrt{46}+5}{3} = 3 + \qquad 17 : 3$$

$$\frac{\sqrt{46}+4}{10} = 1 + \qquad 62 : 11$$

$$\frac{\sqrt{46}+6}{1} = 12 + \qquad 79 : 14$$

Cette dernière fraction convergente $\frac{79}{14}$ satisfait à l'équation proposée, parce qu'elle est de rang impair, et qu'ainsi on a $pq^{\circ} - p^{\circ}q = +1$. Maintenant, suivant la remarque qui a été faite dans le cas précédent, on supposera que le quotient qui répond à la dernière fraction convergente $\frac{79}{14}$ est $6 + \frac{\Phi}{\Psi}$, et on en conclura la fraction suivante $\frac{y}{z} = \frac{79\left(6+\frac{\Phi}{\Psi}\right)+62}{14\left(6+\frac{\Phi}{\Psi}\right)+11} = \frac{79\Phi + 536\Psi}{14\Phi + 95\Psi}$; d'où résultera généralement $y = 79\Phi \pm 536\Psi$, $z = 14\Phi \pm 95\Psi$, et ainsi la troisième solution sera

$$x = 268\Phi \pm 1817\Psi$$
$$y = 79\Phi \pm 536\Psi.$$

(76) Soit 4°. $n = 43$ et $x = 43y - 105z$, la transformée sera $35yy - 172yz + 210z^2 = 1$. Il faut donc développer une racine de l'équation $35x^2 - 172x + 210 = 0$, jusqu'à ce qu'on trouve un

quotient-complet $\frac{\sqrt{46}+I}{D}$ dans lequel $D$ soit égal à l'unité. Voici l'opération :

| | |
|---|---|
| $x=\frac{\sqrt{46}+86}{35}=2+$ | 1 : 0 |
| $\frac{\sqrt{46}-16}{-6}=1+$ | 2 : 1 |
| $\frac{\sqrt{46}+10}{9}=1+$ | 3 : 1 |
| $\frac{\sqrt{46}-1}{5}=1+$ | 5 : 2 |
| $\frac{\sqrt{46}+6}{2}=6+$ | 8 : 3 |
| $\frac{\sqrt{46}+6}{5}=2+$ | 53 : 20 |
| $\frac{\sqrt{46}+4}{6}=1+$ | 114 : 43 |
| $\frac{\sqrt{46}+2}{7}=1+$ | 167 : 63 |
| $\frac{\sqrt{46}+5}{3}=3+$ | 281 : 106 |
| $\frac{\sqrt{46}+4}{10}=1+$ | 1010 : 381 |
| $\frac{\sqrt{46}+6}{1}=12+$ | 1291 : 487 |

Cette onzième fraction convergente satisfait à l'équation proposée $35y^2-172yz+210z^2=+1$, puisqu'elle est de rang impair ; ensuite on aura la solution complète, en mettant $6+\frac{\Phi}{\Psi}$ à la place du quotient correspondant, ce qui donnera

$$\frac{y}{z}=\frac{1291\left(6+\frac{\Phi}{\Psi}\right)+1010}{487\left(6+\frac{\Phi}{\Psi}\right)+381}=\frac{1291\,\Phi+8756\,\Psi}{487\,\Phi+3303\,\Psi};$$

d'où résultera la quatrième solution

$$x=4378\,\Phi\pm 29693\,\Psi$$
$$y=1291\,\Phi\pm\ 8756\,\Psi.$$

(77) Il est bon de remarquer qu'on seroit parvenu plus promptement et plus simplement au même résultat, en développant l'autre racine de la même équation. Voici l'opération :

$$x=\frac{\sqrt{46}-86}{-35}=2+ \qquad 1 : 0$$

$$\frac{\sqrt{46}+16}{6}=3+ \qquad 2 : 1$$

$$\frac{\sqrt{46}+2}{7}=1+ \qquad 7 : 3$$

$$\frac{\sqrt{46}+5}{3}=3+ \qquad 9 : 4$$

$$\frac{\sqrt{46}+4}{10}=1+ \qquad 34 : 15$$

$$\frac{\sqrt{46}+6}{1}=12+ \qquad 43 : 19.$$

De-là résulte $\frac{y}{z}=\frac{43\left(6+\frac{\Phi}{\Psi}\right)+34}{19\left(6+\frac{\Phi}{\Psi}\right)+15}=\frac{43\Phi+292\Psi}{19\Phi+129\Psi}$, et on a pour la quatrième solution

$$x=146\Phi\pm989\Psi$$
$$y=43\Phi\pm292\Psi.$$

Formules qui reviennent au même, et qui sont plus simples que celles qu'on a trouvées par le moyen de l'autre racine. Cette identité au reste se démontre, en supposant que les $\Phi$ et $\Psi$ de cette formule répondent à une valeur de $n$ moindre d'une unité que les $\Phi$ et $\Psi$ de l'autre formule ; de sorte qu'en distinguant ceux-ci par $\Phi'$ et $\Psi'$, on pourroit faire $\Phi+\Psi\sqrt{46}=(\Phi'+\Psi'\sqrt{46})(24335\mp3588\sqrt{46})$.

Rassemblant ces différens résultats, on aura toutes les solutions de l'équation proposée $2x^2-23y^2=105$ contenues dans les formules suivantes, où l'on suppose $(24335+3588\sqrt{46})^n=\Phi+\Psi\sqrt{46}$

$$x=8\Phi\pm23\Psi, \quad y=\Phi\pm16\Psi$$
$$x=38\Phi\pm253\Psi, \quad y=11\Phi\pm76\Psi$$
$$x=268\Phi\pm1817\Psi, \quad y=79\Phi\pm536\Psi$$
$$x=146\Phi\pm989\Psi, \quad y=43\Phi\pm292\Psi.$$

La même équation, ou une équation équivalente $(p^2-46q^2=210)$ est résolue dans les Mémoires de Berlin année 1767, et le résultat donné page 263 présente huit solutions.

Ces huit solutions se réduisent aux quatre précédentes ; et en général, le calcul peut toujours s'abréger de moitié, en observant, comme nous l'avons fait, qu'il est inutile de développer en fraction continue les deux racines de la même équation, et que le développement d'une seule suffit pour avoir le résultat des deux.

(78) Prenons encore pour exemple l'équation

$$67y^2-227yz+191z^2=5,$$

laquelle étant comparée à la formule générale (n°. 59) donne $f=67$, $g=-227$, $h=191$, $D=5$, $A=\frac{g^2}{4}-fh=\frac{341}{4}$, et $D<\sqrt{A}$. Donc on peut résoudre cette équation par le développement d'une racine de l'équation $67x^2-227x+191=0$ en fraction continue. Voici l'opération prolongée jusqu'à ce qu'on ait trouvé la période qui se répète à l'infini :

| | | | |
|---|---|---|---|
| | $x=\frac{113\frac{1}{2}+\frac{1}{2}\sqrt{341}}{67}=1+$ | 1 : 0 | |
| | $\frac{-46\frac{1}{2}+\frac{1}{2}\sqrt{341}}{-31}=1+$ | 1 : 1 | |
| | $\frac{15\frac{1}{2}+\frac{1}{2}\sqrt{341}}{5}=4+$ | 2 : 1 | * |
| * | $\frac{4\frac{1}{2}+\frac{1}{2}\sqrt{341}}{13}=1+$ | 9 : 5 | |
| | $\frac{8\frac{1}{2}+\frac{1}{2}\sqrt{341}}{1}=17+$ | 11 : 6 | |
| | $\frac{8\frac{1}{2}+\frac{1}{2}\sqrt{341}}{13}=1+$ | 196 : 107 | |
| | $\frac{4\frac{1}{2}+\frac{1}{2}\sqrt{341}}{5}=2+$ | 207 : 113 | * |
| | $\frac{5\frac{1}{2}+\frac{1}{2}\sqrt{341}}{11}=1+$ | 610 : 333 | |
| | $\frac{5\frac{1}{2}+\frac{1}{2}\sqrt{341}}{5}=2+$ | 817 : 446 | * |
| * | $\frac{4\frac{1}{2}+\frac{1}{2}\sqrt{341}}{13}=1+$ | &c. | |

Le quotient-complet $\frac{4\frac{1}{2}+\frac{1}{2}\sqrt{341}}{13}$ étant un de ceux qui ont été déjà trouvés, l'opération est terminée, et on voit qu'immédiatement après les premiers termes 1, 1, 4, on a la période 1, 17, 1, 2, 1, 2, laquelle se répète à l'infini.

Si on cherche maintenant le nombre 5 parmi les dénominateurs des quotiens-complets, on verra que la troisième fraction convergente, la septième et la neuvième, peuvent satisfaire à l'équation proposée. La septième et la neuvième comprises dans une même période, satisfont en effet, parce qu'elles sont de rang impair, et que dans la valeur de $x$ le radical a été pris en plus. Quant à la troisième, elle satisfait aussi; mais nous en ferons abstraction, parce qu'il suffit de considérer les solutions données par les termes d'une même période, et que toutes les autres doivent y être contenues. Voyez à ce sujet le paragraphe suivant.

On aura donc, par la septième fraction convergente, $p=207$, $q=113$, et calculant à l'ordinaire la valeur de la période comptée depuis ce terme :

Période...... 2, 1, 2, 1, 17, 1

Fract. converg. $\frac{1}{0}$, $\frac{2}{1}$, $\frac{3}{1}$, $\frac{8}{3}$, $\frac{11}{4}$, $\frac{195}{71}$, $\frac{206}{75}$

on trouve $\frac{\alpha}{\mathcal{C}}=\frac{206}{75}$, $\mathcal{C}=71$, $\varphi=\frac{\alpha+\mathcal{C}}{2}=138\frac{1}{2}$, $\psi=\frac{\mathcal{C}}{D}=15$, donc on aura

$$\left(\frac{277}{2}+\frac{15}{2}\sqrt{341}\right)^2=\Phi+\tfrac{1}{2}\Psi\sqrt{341}.$$

Or on a en même temps $\varphi^2-A\psi^2=+1$, ce qui prouve que l'équation proposée est résoluble avec le second membre $+5$; mais elle ne le seroit pas avec le second membre $-5$. Cela posé, en substituant les valeurs trouvées dans la formule du n°. 59, on aura pour première solution de l'équation proposée

$$y=207\Phi\pm3823.\tfrac{1}{2}\Psi$$
$$z=113\Phi\pm2087.\tfrac{1}{2}\Psi.$$

Procédant de la même manière à l'égard de la neuvième fraction convergente $\frac{817}{446}$, on en déduira cette seconde solution :

$$y=817\Phi\pm15087.\tfrac{1}{2}\Psi$$
$$z=446\Phi\pm8236.\tfrac{1}{2}\Psi.$$

Ces dernières formules sont celles qui contiennent la solution $\frac{2}{1}$ que nous avons remarquée dans la partie irrégulière de la fraction continue. En effet si on suppose $n=1$, $\Phi=\frac{277}{2}$, $\pm\Psi=-15$, on trouvera $y=2$, $z=1$. De-là on peut présumer que la seconde solution générale est susceptible de se rédnire à une forme plus simple, et c'est de quoi on s'assurera aisément, en prenant au lieu de $\Phi$ et $\Psi$ les quantités analogues qui répondent à une valeur de $n$ différente d'une unité. Il en résultera

$$y = 2\Phi \pm 72.\tfrac{1}{2}\Psi$$
$$z = \Phi \pm 41.\tfrac{1}{2}\Psi.$$

(79) On voit, par ce qui a été démontré dans ce paragraphe, que lorsque les équations qui en font l'objet sont possibles, leur résolution est donnée par un ou plusieurs systêmes de formules telles que

$$y = a'\Phi + b'\Psi$$
$$z = a''\Phi + b''\Psi,$$

les nombres $a'$, $b'$, $a''$, $b''$ étant constans, et les quantités $\Phi$, $\Psi$ étant tirées de l'équation

$$(\varphi + \psi\sqrt{A})^n = \Phi + \Psi\sqrt{A},$$

dans laquelle $n$ est un nombre indéterminé, et où l'on a toujours $\varphi^2 - A\psi^2 = \pm 1$, et par conséquent aussi $\Phi^2 - A\Psi^2 = (\pm 1)^n = +1$ ou $-1$.

Dans les formules générales, on peut prendre $\Psi$ négatif ou positif à volonté, et ainsi affecter $\Psi$ du double signe $\pm 1$; ce qui revient à laisser le signe de $\Psi$ déterminé, mais à prendre pour $n$ des valeurs quelconques tant positives que négatives. En effet on a $(\varphi+\psi\sqrt{A})^{-n} = (\varphi^2 - A\psi^2)^{-n}(\varphi - \psi\sqrt{A})^n = (\pm 1)^n(\Phi - \Psi\sqrt{A})$, et ainsi le changement du signe de $n$ revient au même que celui du signe de $\Psi$; car d'ailleurs le signe de $(\pm 1)^n$ qui affecte le tout est indifférent, puisque par la nature de l'équation proposée on peut changer à-la-fois le signe de $y$ et celui de $z$.

Il résulte de-là que les diverses valeurs de $y$ et $z$ comprises dans un systême de formules, tel que le précédent, forment deux suites qui s'étendent à l'infini, tant dans le sens positif que dans le

le sens négatif, et dont chaque terme répond à une valeur déterminée de $n$ positive ou négative, en cette sorte :

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $n$ | .... &c. | $-3$, | $-2$, | $-1$, | $0$, | $1$, | $2$, | $3$, | &c. |
| $y$ | &c. | $'''p$, | $''p$, | $'p$, | $p$, | $p1$, | $p2$, | $p3$, | &c. |
| $z$ | &c. | $'''q$, | $''q$, | $'q$, | $q$, | $q1$, | $q2$, | $q3$, | &c. |

Au reste, la manière la plus simple de calculer les valeurs numériques de ces termes, est de faire usage de la loi trouvée n°. 54, laquelle donnera $p2 = 2\varphi p1 \mp p$ (le signe $\mp$ étant le contraire de celui de $\varphi^2 - A\psi^2$). Cette formule où $p$, $p1$, $p2$ désignent en général trois termes consécutifs, peut servir à prolonger l'une des séries, soit à droite, soit à gauche, et la même loi a lieu dans l'autre série.

## §. XII. *Démonstration d'une proposition supposée dans les paragraphes précédens.*

(80) Nous avons supposé jusqu'ici que s'il est possible de satisfaire à l'équation $fy^2+gyz+hz^2=\pm H$, où l'on suppose $y$ et $z$ premiers entr'eux, et $H<\frac{1}{2}\sqrt{(g^2-4fh)}$, la fraction $\frac{y}{z}$ est toujours comprise parmi les fractions convergentes vers une racine de l'équation $fx^2+gx+h=0$. Cette proposition a beaucoup d'analogie avec celle du n°. 10, mais il n'est pas moins nécessaire de démontrer qu'elle est vraie généralement, sauf une légère exception dont nous ferons mention.

Soit $f$ un nombre positif, $g$ et $h$ des nombres positifs ou négatifs à volonté; soit $\frac{p}{q}$ une fraction donnée dont les termes sont premiers entr'eux, et satisfont à l'équation

$$fp^2+gpq+hq^2=\pm H,$$

je suppose qu'on développe $\frac{p}{q}$ en fraction continue, et que les quotiens qui résultent de cette opération soient $\alpha$, $\beta$,.... $\lambda$, $\mu$. Au moyen de ces quotiens, on calculera à l'ordinaire les fractions convergentes vers $\frac{p}{q}$, et en désignant par $\frac{p^\circ}{q^\circ}$ celle qui précède immédiatement $\frac{p}{q}$, nous avons déjà vu (n°. 9) qu'on peut faire à volonté $pq^\circ-p^\circ q=+1$, ou $pq^\circ-p^\circ q=-1$.

Cela posé, considérons les mêmes fractions consécutives $\frac{p^\circ}{q^\circ}$, $\frac{p}{q}$ comme appartenant au développement de $x$ en fraction continue; soit $z$ le quotient-complet qui répond à la dernière, il faudra donc qu'on ait $x=\frac{pz+p^\circ}{qz+q^\circ}$, ou $z=\frac{q^\circ x-p^\circ}{p-qx}$. Maintenant la supposition faite que $\frac{p^\circ}{q^\circ}$, $\frac{p}{q}$ sont deux fractions consécutives convergentes

vers $x$, sera légitime, si la valeur de $z$ qu'on vient de trouver est positive et plus grande que l'unité; car telle est la condition à laquelle doivent être soumis tous les quotiens-complets qui résultent du développement d'une quantité quelconque en fraction continue. Il s'agit donc d'examiner si cette condition est remplie.

De l'équation précédente on tire $z + \frac{q^{\circ}}{q} = \frac{pq^{\circ} - p^{\circ}q}{q^{\circ}\left(\frac{p}{q} - x\right)}$, or en faisant toujours $A = \frac{1}{4}g^2 - fh$, on a $x = \frac{-\frac{1}{2}g \pm \sqrt{A}}{f}$; substituant cette valeur à la place de $x$, et faisant passer le radical au numérateur, on aura

$$z + \frac{q^{\circ}}{q} = \frac{pq^{\circ} - p^{\circ}q}{2} \quad . \quad \frac{2f\frac{p}{q} + g \mp 2\sqrt{A}}{fp^2 + gpq + hq^2}.$$

Dans cette équation, on peut prendre à volonté le signe de $\sqrt{A}$, parce qu'on est maître de prendre pour $x$ l'une ou l'autre racine de l'équation $fx^2 + gx + h = 0$, et la valeur de $z$ est différente dans les deux cas; en même temps, puisqu'on a $fp^2 + gpq + hq^2 = \pm H$, cette équation donnera

$$\frac{2fp}{q} + g = \pm 2\sqrt{\left(A \pm \frac{fH}{qq}\right)};$$

par conséquent on aura

$$z + \frac{q^{\circ}}{q} = (pq^{\circ} - p^{\circ}q) \quad . \quad \frac{\pm\sqrt{A} \pm \sqrt{\left(A \pm \frac{fH}{qq}\right)}}{\pm H}.$$

De ces diverses indéterminations de signes il n'y a que celle de $\pm\sqrt{A}$ qui soit arbitraire, car celle de $H$ dépend de l'équation proposée, et celle de $\sqrt{\left(A \pm \frac{fH}{qq}\right)}$ est également fixée par la valeur de $\frac{2fp}{q} + g$. Mais comme il importe de considérer la valeur la plus grande de $z$, on prendra le signe de $\sqrt{A}$ pareil à celui de $\sqrt{\left(A \pm \frac{fH}{q^2}\right)}$, et alors le second membre de notre équation sera nécessairement de la forme

$$\pm(pq^{\circ} - p^{\circ}q) \quad . \quad \frac{\sqrt{A} + \sqrt{\left(A \pm \frac{fH}{q^2}\right)}}{H}.$$

Enfin on pourra toujours supposer cette quantité positive, puisqu'on peut faire à volonté $pq^\circ - p^\circ q = +1$ ou $-1$; donc on aura dans tous les cas

$$z + \frac{q^\circ}{q} = \frac{\sqrt{A} + \sqrt{\left(A \pm \frac{fH}{qq}\right)}}{H}.$$

(81) Soit 1°. $fp^2 + gpq + hq^2 = +H$, et on aura

$$z + \frac{q^\circ}{q} = \frac{\sqrt{A} + \sqrt{\left(A + \frac{fH}{qq}\right)}}{H}.$$

Le second membre est plus grand que $\frac{2\sqrt{A}}{H}$, et par conséquent $>2$, puisqu'on a $H < \sqrt{A}$; d'ailleurs $q^\circ$ est $< q$; donc la valeur de $z$ est positive et plus grande que l'unité. Donc la fraction donnée $\frac{p}{q}$ qui satisfait à l'équation $fp^2 + gpq + hq^2 = +H$, est toujours l'une des fractions convergentes vers une racine de l'équation $fx^2 + gx + h = 0$, et cette conclusion ne souffre aucune exception tant que le second membre $H$ est positif.

(82) Soit 2°. $fp^2 + gpq + hq^2 = -H$, on aura

$$z + \frac{q^\circ}{q} = \frac{\sqrt{A} + \sqrt{\left(A - \frac{fH}{qq}\right)}}{H}.$$

Or on voit que pour peu que $q^2$ soit grand par rapport à $\frac{fH}{A}$, (et il ne peut jamais être moindre) la valeur de $z + \frac{q^\circ}{q}$ sera à très-peu-près égale à $\frac{2\sqrt{A}}{H}$, de sorte qu'on aura $z = \frac{2\sqrt{A}}{H} - \frac{q^\circ}{q}$, quantité positive et plus grande que l'unité.

Au reste, sans négliger le terme $\frac{fH}{qq}$, il est facile d'assigner la limite de $q$, telle qne $z$ soit encore positive et plus grande que l'unité. Pour cela mettons $z$ sous la forme

$$z = \frac{2\sqrt{A}}{H} - \left(\frac{1 + q^\circ}{q}\right) + \frac{1}{q} - \frac{\sqrt{A}}{H} + \frac{1}{H}\sqrt{\left(A - \frac{fH}{qq}\right)}:$$

à cause de $\sqrt{A} > H$, $\frac{1+q^2}{q} < 1$ ou tout au plus $=1$. Il est clair que $z$ sera positif et plus grand que l'unité, si la quantité $\sqrt{\left(A - \frac{fH}{qq}\right)}$ est plus grande que $\sqrt{A} - \frac{H}{q}$. Soit donc $\sqrt{\left(A - \frac{fH}{qq}\right)} > \sqrt{A} - \frac{H}{q}$; de-là on tire en quarrant et réduisant

$$q > \frac{f+H}{2\sqrt{A}}.$$

Donc tant qu'on aura $q$ au-dessus de cette limite, il est certain que la valeur de $z$ sera toujours plus grande que l'unité; mais si on a $q < \frac{f+H}{2\sqrt{A}}$, on ne peut plus affirmer en général que $z$ soit plus grande que l'unité.

(83) Quel que soit $q$, l'exception n'aura jamais lieu, lorsque $f$ étant, comme nous le supposons, un nombre positif, $h$ est un nombre négatif, car alors l'équation proposée aura la forme

$$fp^2 + gpq - h'q^2 = -H,$$

laquelle est la même que

$$h'q^2 - gpq - fp^2 = +H.$$

Cette équation étant ainsi ramenée au premier cas, il s'ensuit que $\frac{q}{p}$ est une fraction convergente vers une racine de l'équation $h'x^2 - gx - f = 0$; donc (en mettant $\frac{1}{x}$ à la place de $x$) $\frac{p}{q}$ sera une fraction convergente vers une racine de l'équation $fx^2 + gx - h' = 0$.

(84) Si on a à résoudre l'équation $fy^2 + gyz + hz^2 = -H$ dans laquelle $f$ et $h$ sont positifs, on pourra toujours (n°. 50) transformer cette équation en une autre $a'y'^2 + by'z' - c'z'^2 = -H$ dans laquelle $a$ et $c$ seront positifs, et où l'on aura $bb + 4ac = gg - 4fh = 4A$. Cette équation sera donc dans le cas du n°. précédent, et si d'ailleurs on a $H < \sqrt{A}$, toutes ses solutions seront données par les fractions convergentes vers une racine de l'équation $ax^2 + bx - c = 0$.

On voit par-là, que l'exception dont nous avons fait mention, et qui d'ailleurs n'a lieu que très-rarement et pour de très-petites valeurs de $p$ et $q$, peut être entièrement évitée par les transfor-

mations déjà indiquées. Il est donc vrai de dire généralement, que lorsque $H$ est $< \frac{1}{2}\sqrt{(gg-4fh)}$, toutes les solutions de l'équation

$$fy^2+gyz+hz^2=\pm H$$

sont données par les fractions convergentes vers une racine de l'équation $fx^2+gx+h=0$.

(85) Il ne sera pas inutile, au reste, d'apporter un exemple sujet à l'exception mentionnée, et qui nous fournira de nouvelles remarques. Soit pour cet effet l'équation

$$1801\,y^2-3991\,yz+2211\,z^2=-3,$$

dans laquelle on a $A=\frac{1}{4}g^2-fh=\frac{37}{4}$, $H=3$, et par conséquent $H<\sqrt{A}$; on satisfait à cette équation en faisant $y=31$ et $z=28$; cependant la fraction $\frac{31}{28}$ n'est point comprise parmi les fractions convergentes vers une racine de l'équation

$$1801\,x^2-3991\,x+2211=0.$$

En effet, le développement de la plus grande racine donne

$$x=\frac{1995\frac{1}{2}+\frac{1}{2}\sqrt{37}}{1801}=1+ \qquad 1 : 0$$

$$\frac{-194\frac{1}{2}+\frac{1}{2}\sqrt{37}}{-21}=9+ \qquad 1 : 1$$

$$\frac{5\frac{1}{2}+\frac{1}{2}\sqrt{37}}{1}=8+ \qquad 10 : 9$$

$$\frac{2\frac{1}{2}+\frac{1}{2}\sqrt{37}}{3}=1+ \qquad 81 : 73$$

&c. &c.

et celui de la plus petite racine donne

$$x=\frac{-1995\frac{1}{2}+\frac{1}{2}\sqrt{37}}{-1801}=1+ \qquad 1 : 0$$

$$\frac{194\frac{1}{2}+\frac{1}{2}\sqrt{37}}{21}=9+ \qquad 1 : 1$$

$$\frac{-5\frac{1}{2}+\frac{1}{2}\sqrt{37}}{-1}=2+ \qquad 10 : 9$$

$$\frac{3\frac{1}{2}+\frac{1}{2}\sqrt{37}}{3}=2+ \qquad 21 : 19$$

$$\frac{2\frac{1}{2}+\frac{1}{2}\sqrt{37}}{1}=5+ \qquad 52 : 47$$

&c. &c.

On ne trouve donc ni d'un côté ni de l'autre la fraction convergente $\frac{31}{28}$; c'est au reste ce qui s'accorde avec la formule de l'art. 82, car ici 28, qui est la valeur de $q$, est plus petit que $\frac{f+H}{2\sqrt{A}}$ qui est $\frac{1804}{\sqrt{37}}$.

(86) Pour éviter cet inconvénient, et pour faire en sorte que la solution soit donnée par les fractions convergentes, il suffit de réduire la quantité $1801y^2-3991yz+2211z^2$, si ce n'est à l'expression la plus simple, au moins à une forme où les termes extrêmes soient de signes contraires. C'est ce qu'on obtient immédiatement en faisant

$$y=10y'-51z'$$
$$z=9y'-46z';$$

car alors l'équation proposée se réduit à cette forme très-simple

$$y'y'+y'z'-9z'z'=-3.$$

Développant donc une racine de l'équation $x^2+x-9=0$ en fraction continue, on aura

$$x=\frac{-\frac{1}{2}+\frac{1}{2}\sqrt{37}}{1}=2+ \qquad 1:0$$
$$* \quad \frac{2\frac{1}{2}+\frac{1}{2}\sqrt{37}}{3}=1+ \qquad 2:1$$
$$\frac{\frac{1}{2}+\frac{1}{2}\sqrt{37}}{3}=1+ \qquad 3:1$$
$$\frac{2\frac{1}{2}+\frac{1}{2}\sqrt{37}}{1}=5+ \qquad 5:2$$
$$* \quad \frac{2\frac{1}{2}+\frac{1}{2}\sqrt{37}}{3}=1+ \qquad 28:11$$

&c. &c.

A l'inspection des quotiens-complets, on voit que la fraction convergente $\frac{2}{1}$ peut être prise pour $\frac{y'}{z'}$, car en faisant $y'=2$, $z'=1$, on a $y'y'+y'z'-9z'z'=-3$; de-là résulte $y=-31$ et $z=-28$; c'est la solution qu'il s'agissoit de trouver par les fractions convergentes.

Au reste, la solution générale de l'équation en $y'$ et $z'$ déduite du développement qu'on vient de faire, est comprise dans les formules suivantes :

1°. Si l'on fait $(6+\sqrt{37})^{2k}=F+G\sqrt{37}$, on aura

$$y'=2F\pm 16G$$
$$z'=F\pm 5G;$$

d'où résulte

$$y=-31F\mp 95G$$
$$z=-28F\mp 86G.$$

2°. Si l'on fait $(6+\sqrt{37})^{2k+1}=F'+G'\sqrt{37}$, on aura

$$y'=3F'\pm 15G'$$
$$z'=F'\pm 7G',$$

et il en résultera

$$y=-21F'\mp 207G'$$
$$z=-19F'\mp 187G'.$$

(87) Si on réfléchit maintenant sur le procédé que nous venons de suivre dans cet exemple, on verra qu'après avoir simplifié la forme de l'équation à résoudre, les solutions les plus simples ont dû se présenter les premières parmi les fractions convergentes, et de ces premières solutions on a conclu par les formules ordinaires la solution générale, qui n'est autre chose que l'expression des diverses fractions convergentes qui satisfont à la question, ces fractions étant prises successivement à la même place dans toutes les périodes. Or l'expression générale ainsi trouvée, par quelque moyen qu'on y soit parvenu, est une ; elle seroit la même au fond, quand pour la trouver on seroit parti des valeurs particulières de $p$ et $q$ dans une autre période que la première. Pour nous faire mieux entendre, prenons l'équation $y^2-3z^2=1$, à laquelle on satisfait par les valeurs successives

$$\frac{y}{z}=\frac{2}{1},\ \frac{7}{4},\ \frac{26}{15},\ \frac{97}{56},\ \frac{362}{209},\ \&c.$$

L'expression générale de ces valeurs, en partant de la première solution $\frac{2}{1}$, seroit $y=F$, $z=G$, $F$ et $G$ étant déterminées par l'équation

l'équation $(2+\sqrt{3})^n = F + G\sqrt{3}$. Mais on peut partir également de la valeur particulière $\frac{26}{15}$, et l'expression générale se tireroit de l'équation $y + z\sqrt{3} = (26 + 15\sqrt{3})\ (F \pm G\sqrt{3})$, laqnelle donne

$$y = 26\,F \pm 45\,G$$
$$z = 15\,F \pm 26\,G.$$

Or cette expression contient non-seulement les nombres supérieurs à 26 et 15, mais tous les inférieurs qui peuvent satisfaire; et en effet, si on prend $F = 2$, $G = 1$, et qu'on emploie le signe inférieur, on aura $y = 52 - 45 = 7$, et $z = 30 - 26 = 4$, c'est la solution qui précède $\frac{26}{15}$; de même en faisant $n = 2$, ou $F = 7$, $G = 4$, et prenant encore le signe inférieur, on aura

$$y = 182 - 180 = 2,\ z = 105 - 104 = 1.$$

Donc toutes les solutions, en grands ou en petits nombres, sont également comprises dans l'expression générale, quelles que soient les valeurs particulières qui ont servi à composer ces formules.

Cela posé, il n'est nécessaire, dans aucun cas, de transformer l'équation proposée $fy^2 + gyz + hz^2 = \pm H$, et on peut se borner à suivre la méthode ordinaire indiquée dans le paragraphe précédent: après avoir développé en fraction continue, conformément à cette méthode, une seule racine de l'équation $fx^2 + gx + h = 0$, et avoir continné le développement, jusqu'à ce que la première période de quotiens soit complète, la considération de cette première période suffit pour avoir l'expression générale des diverses fractions convergentes qui dans les périodes successives peuvent satisfaire à l'équation proposée. Et on peut être assuré que les formules ainsi trouvées contiennent absolument toutes les solutions, même celles qui, à canse de l'irrégularité de la fraction continue dans ses premiers termes, ne se trouvent point comprises parmi les fractions convergentes.

(88) Ainsi, pour résoudre l'équation $1801\,y^2 - 3991\,yz + 2211\,z^2 = -3$, on développera simplement une racine de l'éqnation $1801\,x^2 - 3991\,x + 2211 = 0$. Voici l'opération continuée jusqu'à

ce que le retour du même quotient-complet manifeste l'étendue de la période

| | |
|---|---|
| $x = \frac{1995\frac{1}{2} + \frac{1}{2}\sqrt{37}}{1801} = 1 +$ | 1 : 0 |
| $\frac{-194\frac{1}{2} + \frac{1}{2}\sqrt{37}}{-21} = 9 +$ | 1 : 1 |
| $\frac{5\frac{1}{2} + \frac{1}{2}\sqrt{37}}{1} = 8 +$ | 10 : 9 |
| $\frac{2\frac{1}{2} + \frac{1}{2}\sqrt{37}}{3} = 1 +$ | 81 : 73 |
| $\frac{\frac{1}{2} + \frac{1}{2}\sqrt{37}}{3} = 1 +$ | 91 : 82 |
| $\frac{2\frac{1}{2} + \frac{1}{2}\sqrt{37}}{1} = 5 +$ | 172 : 155 |
| $\frac{2\frac{1}{2} + \frac{1}{2}\sqrt{37}}{3} = 1 +$ | 951 : 857 |
| &c. | &c. |

On voit que la période qui se répète sans cesse est 1, 1, 5; et en appliquant les formules du paragraphe IX, on trouvera que la solution déduite de la fraction $\frac{81}{73}$ est, en supposant $(6+\sqrt{37})^{2k} = F+G\sqrt{37}$,

$$y = 81\,F \mp 465\,G$$
$$z = 73\,F \mp 419\,G,$$

et la solution déduite de la fraction $\frac{91}{82}$ sera, en supposant $(6+\sqrt{37})^{2k+1} = F'+G'\sqrt{37}$,

$$y = 91\,F' \mp 577\,G'$$
$$z = 82\,F' \mp 520\,G'.$$

Si dans cette dernière on fait $F'=6$, et $G'=1$, on aura, en prenant le signe supérieur, $y=-31$, $z=-28$.

Or il est facile de s'assurer que ces formules s'accordent avec celles qu'on a trouvées n°. 86. Il suffit pour cela de mettre, au lieu de $F'$ et $G'$, leurs valeurs tirées de l'équation $F'+G'\sqrt{37} = (6\pm\sqrt{37})(F+G\sqrt{37})$, savoir $F'=6F\pm37G$, $G'=6G\pm F$.

## §. XIII. *Réduction ultérieure des formules* $Ly^2+Myz+Nz^2$ *lorsque* $M^2-4LN$ *est égal à un nombre positif.*

(89) Supposons d'abord que le coefficient $M$ est pair, et soit la formule proposée $py^2+2qyz+rz^2$; nous avons vu (n°. 46) que si $q^2-pr$ est égal à un nombre positif $A$, cette formule peut toujours se réduire à la forme $ay^2+2byz-cz^2$, dans laquelle $a$ et $c$ sont toujours positifs, non moindres que $2b$, et où l'on a $b^2+ac=A$. Nous nous proposons maintenant de réduire au plus petit nombre possible les diverses formules $ay^2+2byz-cz^2$ qui pour un nombre donné $A$ satisfont aux conditions précédentes. Faisons voir d'abord comment on trouve ces formules.

Soit par exemple $A=79=b^2+ac$, on donnera à $b$ les valeurs successives 0, 1, 2, 3, sans aller plus loin, parce que $b$ doit être $<\sqrt{\frac{79}{5}}$. Chaque valeur de $b$ en fera connoître une de $ac=79-b^2$, mais celle-ci ne peut être utile qu'autant qu'elle pourra être décomposée en deux facteurs qui ne soient pas moindres que $2b$. Voici le détail du calcul où l'on a supposé constamment $a<c$:

1°. $\begin{cases} b=0 \\ ac=79 \\ a>0 \end{cases}$ $\quad a=1, \quad c=79$

2°. $\begin{cases} b=1 \\ ac=78 \\ a>2 \end{cases}$ $\quad a=2, \quad c=39$; $\quad 3, \quad 26$; $\quad 6, \quad 13$

3°. $\begin{cases} b=2 \\ ac=75 \\ a>4 \end{cases}$ $\quad a=5, \quad c=15$

4°. $\begin{cases} b=3 \\ ac=70 \\ a>6. \end{cases}$ $\quad a=7, \quad c=10$

De-là on voit que toute quantité indéterminée $py^2+2qyz+rz^2$, dans laquelle $q^2-pr=79$, doit se réduire à l'une des douze formes suivantes :

| | |
|---|---|
| $y^2-79z^2$ | $79y^2-z^2$ |
| $2y^2+2yz-39z^2$ | $39y^2+2yz-2z^2$ |
| $3y^2+2yz-26z^2$ | $26y^2+2yz-3z^2$ |
| $6y^2+2yz-13z^2$ | $13y^2+2yz-6z^2$ |
| $5y^2+4yz-15z^2$ | $15y^2+4yz-5z^2$ |
| $7y^2+6yz-10z^2$ | $10y^2+6yz-7z^2$ |

De ces douze formes il y en a six qui ne sont autre chose que les six autres prises avec des signes contraires, car d'ailleurs la forme $ay^2+2byz-cz^2$ ne diffère pas de $ay^2-2byz-cz^2$, puisqu'on peut prendre indifféremment $z$ positif ou négatif.

(90) Il pourra arriver pour certaines valeurs de $A$, qu'une formule $ay^2+2byz-cz^2$ soit identique avec son inverse $cy^2+2byz-az^2$, et c'est ce qui aura toujours lieu, si on peut satisfaire à l'équation $m^2-An^2=-1$. En effet, si l'on a $m^2-An^2=-1$, et qu'on fasse $ay^2+2byz-cz^2=Z=cz'^2+2by'z'-ay'^2$, ces deux valeurs de $Z$, l'une donnée, l'autre hypothétique, étant multipliées par $a$, on aura, après avoir fait pour abréger, $ay+bz=x$, $ay'+bz'=x'$;

$$aZ=x^2-Az^2$$
$$-aZ=x'^2-Az'^2.$$

D'où, à cause de $-1=m^2-An^2$, on tire

$$x'^2-Az'^2=(m^2-An^2)(x^2-Az^2).$$

Pour satisfaire à cette équation, on peut la décomposer en ces deux autres :

$$x'+z'\sqrt{A}=(m-n\sqrt{A})(x+z\sqrt{A})$$
$$x'-z'\sqrt{A}=(m+n\sqrt{A})(x-z\sqrt{A});$$

desquelles résultent

$$x'=mx-nAz$$
$$z'=mz-nx=(m-bn)z-any.$$

Donc en premier lieu $z'$ est un entier; ensuite si à la place de $x$ et $x'$ on met leurs valeurs $ay+bz$, $ay'+bz'$, on aura après les réductions $y'=(m+bn)y-cnz$. Donc $y'$ est aussi un entier, et

ainsi la formule $ay^2+2byz-cz^2$ est la même que son inverse $cz'^2+2by'z'-ay'^2$.

Lorsque $A$ ne surpasse pas 1003, l'inspection de la table XII fera voir si l'équation $m^2-An^2=-1$ est possible ; elle le sera toujours (n°. 42) lorsque $A$ est un nombre premier $4k+1$, et en général il faut que tous les diviseurs premiers de $A$ ou de $\frac{1}{2}A$ soient de la forme $4k+1$; mais cette condition n'est pas suffisante, puisqu'elle est remplie à l'égard de 34, 146, 205, &c., sans néanmoins que l'équation dont il s'agit soit possible.

(91) Cela posé, voici la méthode pour découvrir parmi toutes les formules qui résultent d'un même nombre $A$, celles qui sont identiques à une formule donnée $ay^2+2byz-cz^2$.

Si la formule $Z=ay^2+2byz-cz^2$ est identique à une autre formule $a'y'^2+2b'y'z'-c'z'^2$, il faudra que celle-ci résulte de la première par quelque transformation. Or la transformation la plus générale consiste à faire (n°. 45)

$$y=py'+p^\circ z'$$
$$z=qy'+q^\circ z',$$

les nombres $p$, $q$, $p^\circ$, $q^\circ$, n'étant pas entièrement arbitraires (1), mais devant satisfaire à la condition $pq^\circ-p^\circ q=\pm 1$. Supposons donc que la substitution de ces valeurs donne $Z=a'y'^2+2b'y'z'-c'z'^2$, nous aurons

$$a'=ap^2+2bpq-cq^2$$
$$b'=app^\circ+b(pq^\circ+p^\circ q)-cqq^\circ$$
$$-c'=ap^{\circ 2}+2bp^\circ q^\circ-cq^{\circ 2}.$$

Maintenant si l'on veut que $a'$ et $-c'$ soient réellement de différens signes, afin que la transformée soit semblable à la formule proposée, il faudra qu'une racine de l'équation $ax^2+2bx-c=0$ tombe entre les deux fractions $\frac{p^\circ}{q^\circ}$, $\frac{p}{q}$; d'ailleurs comme on a $b'b'+a'c'=bb+ac=A$, et qu'ainsi l'un des nombres $a'$ et $c'$ est nécessairement $<\sqrt{A}$, il faut que l'une au moins des deux fractions précédentes soit comprise parmi les fractions convergentes

(1) Les lettres $p$ et $q$ n'ont aucun rapport avec les coefficiens de la forme primitive que nous avions représentée par $py^2+2qyz+rz^2$.

vers la racine $x$. (§. XII.) Soit $\frac{p}{q}$ cette fraction, et soit prise pour $\frac{p^\circ}{q^\circ}$ la fraction convergente qui précède $\frac{p}{q}$, alors les quatre nombres $p$, $q$, $p^\circ$, $q^\circ$ seront déterminés par deux fractions successives résultantes du développement de la racine $x$ en fraction continue. Mais j'observe qu'il n'est pas même nécessaire de calculer ces fractions pour avoir les transformées successives $a'y'^2+2b'y'z'-c'z'^2$. En effet soit $\frac{\sqrt{A}+I}{D}$ le quotient-complet qui répond à la fraction convergente $\frac{p}{q}$, on aura comme il a été trouvé ci-dessus (n°. 51)

$$ap^2+2bpq-cq^2=D(pq^\circ-p^\circ q)$$
$$app^\circ+b(pq^\circ+p^\circ q)-cqq^\circ=-I(pq^\circ-p^\circ q)$$
$$ap^{\circ 2}+2bp^\circ q^\circ-cq^{\circ 2}=-D^\circ(pq^\circ-p^\circ q).$$

Donc la transformée $Z$ sera simplement

$$Z=(pq^\circ-p^\circ q)\ (Dy'^2-2Iy'z'-D^\circ z'^2);$$

et ainsi, de chaque quotient-complet on déduit immédiatement et sans calcul, la transformée correspondante. Il est inutile d'ajouter que dans la première transformée $pq^\circ-p^\circ q$ aura pour valeur $-1$, dans la seconde $+1$, et ainsi alternativement.

(92) Cherchons, par exemple, les transformées dont est susceptible la formule $Z=y^2-79z^2$, il faudra faire la même opération que pour changer en fraction continue une racine de l'équation $x^2-79=0$ : voici cette opération et les transformées qui en résultent :

| | *Transformées.* |
|---|---|
| $x=\sqrt{79}=8+$ | |
| $\frac{\sqrt{79}+8}{15}=1+$ | $-15y'y'+16y'z'+z'z'$ |
| $\frac{\sqrt{79}+7}{2}=7+$ | $2y'y'-14y'z'-15z'z'$ |
| $\frac{\sqrt{79}+7}{15}=1+$ | $-15y'y'+14y'z'+2z'z'$ |
| $\frac{\sqrt{79}+8}{1}=16+$ | $y'y'-16y'z'-15z'z'$ |
| $\frac{\sqrt{79}+8}{15}=1+$ | &c. |

Il est inutile de continuer l'opération plus loin, parce que le retour des mêmes quotiens ramènera les mêmes transformées. On voit donc que de la formule proposée $y^2-79z^2$ il ne résulte que quatre transformées, lesquelles se réduisent aux deux suivantes :

$$2y^2-14yz-15z^2$$
$$y^2+16yz-15z^2.$$

Si ensuite on ramène celles-ci à la forme ordinaire où $2b$ soit $< a$ et $c$, elles deviendront

$$2y^2-2yz-39z^2$$
$$y^2-79z^2;$$

et comme l'une des deux n'est autre que la formule proposée, il n'y a véritablement que $2y^2-2yz-39z^2$ qui en soit une transformée.

(93) Pour réduire les autres formules trouvées (n°. 89) dans le cas de $A=79$, considérons une d'entr'elles $3y^2+2yz-26z^2$, et développons en fraction continue une racine de l'équation $3x^2+2x-26=0$; on trouvera les transformées suivantes, où, pour plus de simplicité, on a supprimé les accens.

| | *Transformées.* |
|---|---|
| $x=\frac{-1+\sqrt{79}}{3}=2+$ | |
| $\frac{\sqrt{79}+7}{10}=1+$ | $-10y^2+14yz+3z^2$ |
| $\frac{\sqrt{79}+3}{7}=1+$ | $7y^2-6yz-10z^2$ |
| $\frac{\sqrt{79}+4}{9}=1+$ | $-9y^2+8yz+7z^2$ |
| $\frac{\sqrt{79}+5}{6}=2+$ | $6y^2-10yz-9z^2$ |
| $\frac{\sqrt{79}+7}{5}=3+$ | $-5y^2+14yz+6z^2$ |
| $\frac{\sqrt{79}+8}{3}=5+$ | $3y^2-16yz-5z^2$ |
| $\frac{\sqrt{79}+7}{10}=$ &c. | &c. |

Ces six transformées réduites à la forme ordinaire (n°. 44) seront

$$3y^2+2yz-26z^2$$
$$7y^2-6yz-10z^2$$
$$7y^2-6yz-10z^2$$
$$-5y^2+4yz+15z^2$$
$$3y^2+2yz-26z^2.$$

De-là il résulte que les douze formes trouvées ci-dessus pour la quantité indéterminée $py^2+2qyz+rz^2$, lorsque $q^2-pr=79$, se réduisent aux quatre suivantes :

$$y^2-79z^2 \qquad 79y^2-z^2.$$
$$3y^2+2yz-26z^2 \qquad 26y^2-2yz-3z^2.$$

Donc toute équation de la forme $py^2+2qyz+rz^2=\pm H$ dans laquelle $q^2-pr=79$, pourra toujours être ramenée à l'une des deux équations

$$y^2-79z^2=\pm H$$
$$3y^2+2yz-26z^2=\pm H.$$

(94) C'est d'après ces principes que nous avons construit la Table I, où l'on trouve pour chaque nombre non quarré $A$ depuis 2 jusqu'à 136, les diverses formes principales auxquelles peuvent toujours se réduire les formules indéterminées $Ly^2+2Myz+Nz^2$ dans lesquelles $M^2-LN=A$. Les signes $\pm$ qui affectent la plupart des formules, indiquent deux formes également possibles, mais qui s'excluent mutuellement. Lorsque les formules ne sont pas précédées d'un signe ambigu, elles ont lieu telles qu'elles sont indiquées, mais elles auroient également lieu avec des signes contraires.

On trouve, par exemple, à côté de 93 la formule réduite $\pm(y^2-93z^2)$; cela signifie que toute formule proposée $py^2+2qyz+rz^2$ dans laquelle $q^2-pr=93$, se réduira toujours à la forme $y'^2-93z'^2$, ou à la forme $93z'^2-y'^2$, mais jamais aux deux à-la-fois.

Au contraire, vis-à-vis de 97 on trouve la formule $y^2-97z^2$ sans ambiguité ; cela signifie que toute formule $py^2+2qyz+rz^2$, dans laquelle $q^2-pr=97$, se réduira toujours à la forme $y'^2-97z'^2$.
Mais

Mais elle se réduiroit aussi, si on vouloit, à la forme $97z'^2-y'^2$, parce que dans ce cas l'équation $m^2-97n^2=-1$ est possible.

(95) Considérons maintenant la formule indéterminée $Ly^2+Myz+Nz^2$ dans laquelle $M$ est impair, et où la quantité $M^2-4LN$ est égale à un nombre positif $B$. Cette formule peut toujours être réduite à la forme $ay^2+byz-cz^2$, où l'on aura à-la-fois $a$ et $c$ positifs, $b<a$ et $c$, et $b^2+4ac=B$. Au moyen du seul nombre $B$, supposé connu, il est facile de trouver toutes les formules $ay^2+byz-cz^2$ qui satisfont aux conditions précédentes; mais ensuite il s'agit de réduire ces formules au moindre nombre possible, en supprimant celles qui sont inutiles ou comprises dans les autres.

Pour cela, considérons l'une de ces formules $ay^2+byz-cz^2$, ou plutôt son double $2ay^2+2byz-2cz^2$; et alors le coefficient du terme moyen étant pair, on pourra procéder, par la méthode précédente, à la recherche de ses transformées successives. Il faudra à cet effet développer en fraction continue une racine de l'équation $2ax^2+2bx-2c=0$, cette racine étant $x=\frac{-b+\sqrt{B}}{2a}$. Les transformées seront également de la forme $2a'y^2+2b'yz-2c'z^2$, laquelle résultera toujours de l'expression

$$(pq^\circ-p^\circ q)\ (Dy^2-2Iyz-D^\circ z^2),$$

et le multiplicateur 2 commun aux unes et aux autres, n'empêchera pas de reconnoître avec une égale facilité les formes identiques.

Il n'y a donc véritablement aucune différence essentielle dans la manière de traiter le cas de $M$ pair et celui de $M$ impair. Mais les résultats de ce dernier cas doivent être consignés dans une table particulière qui offrira pour chaque nombre $B$ de la forme $4n+1$, les formes essentiellement différentes auxquelles se rapportent toutes les formules indéterminées $Ly^2+Myz+Nz^2$ dans lesquelles $M$ est impair et $M^2-4LN=B$.

(96) Pour donner un exemple du calcul de cette table, soit $B=181$. Nous chercherons d'abord les diverses valeurs de $a, b, c$ qui satisfont à l'équation $b^2+4ac=181$, et comme en vertu des autres conditions le nombre impair $b$ doit être $<\sqrt{\frac{181}{5}}$, on fera successivement $b=1, 3, 5$ : ce qui donnera, en supposant $a<c$,

1°. $\begin{cases} b=1 \\ ac=45 \\ a>1 \end{cases}$ $\quad a=1, \quad c=45$; $\quad 3, \quad 15$; $\quad 5, \quad 9$

2°. $\begin{cases} b=3 \\ ac=43 \\ a>3 \end{cases}$ : non décomposable.

3°. $\begin{cases} b=5 \\ ac=39 \\ a>5 \end{cases}$ : non décomposable en facteurs $>5$.

Donc toutes les formules indéterminées $Ly^2+Myz+Nz^2$ dans lesquelles $M^2-4LN=181$, peuvent se réduire à l'une de ces six formes :

$$\pm(y^2+yz-45z^2)$$
$$\pm(3y^2+yz-15z^2)$$
$$\pm(5y^2+yz-9z^2).$$

D'ailleurs puisque 181 est un nombre premier $4n+1$, l'équation $m^2-181n^2=-1$ est possible (n°. 42), et ainsi les six formes précédentes se réduisent à trois, en ôtant le signe ambigu. Il ne reste donc plus qu'à examiner si ces trois formes peuvent se réduire à un moindre nombre.

Pour cela je cherche les transformées de la formule $2y^2+2yz-90z^2$, ce qui se fera, en développant une racine de l'équation fictive $2x^2+2x-90=0$ par le calcul suivant :

| | Transformées. |
|---|---|
| $x=\frac{-1+\sqrt{181}}{2}=6+$ | |
| $\frac{13+\sqrt{181}}{6}=4+$ | $-6y^2+26yz+2z^2$ |
| $\frac{11+\sqrt{181}}{10}=2+$ | $10y^2+22yz-6z^2$ |
| $\frac{9+\sqrt{181}}{10}=2+$ | $-10y^2+18yz+10z^2$ |
| $\frac{11+\sqrt{181}}{6}=4+$ | $6y^2+22yz-10z^2$ |
| $\frac{13+\sqrt{181}}{2}=13+$ | $-2y^2+26yz+6z^2$ |
| $\frac{13+\sqrt{181}}{6}=4+$ | $6y^2+26yz-2z^2$ |
| &c. | &c. |

Il faut ensuite prendre les moitiés de ces transformées, et les réduire à la forme ordinaire, en diminuant le coefficient moyen : or j'observe que cela peut se faire de deux manières tant que le coefficient moyen est plus grand que chacun des extrêmes. Par exemple, dans la première transformée $-3y^2+13yz+z^2$, on peut substituer $y-2z$ à la place de $y$, ce qui donne $-3y^2+yz+15z^2$ ou bien on peut mettre $z-6y$ à la place de $z$, ce qui donnera $z^2+yz-45z^2$. Traitant ainsi les deux premières transformées, et observant que par la nature du nombre 181, il est permis de changer tous les signes de chaque résultat, on trouve qu'elles comprennent à elles seules les trois formes

$$y^2+yz-45z^2$$
$$3y^2-yz-15z^2$$
$$5y^2+yz-9z^2.$$

Donc il est inutile d'avoir égard aux autres transformées, et on a acquis la certitude que la seule forme $y^2+yz-45z^2$ renferme toutes les autres. Donc toute équation indéterminée $Ly^2+Myz+Nz^2=\pm H$ dans laquelle $M^2-4LN=181$, pourra toujours se réduire à la forme $y^2+yz-45z^2=H$.

(97) La Table II offre les réductions de ce genre pour tous les nombres $B$ de forme $4n+1$, depuis 5 jusqu'à 305. Cette table, indépendamment de ses autres usages, pourra faciliter beaucoup la résolution des équations de la forme précédente, dans lesquelles $B$ ne surpasse pas 305.

Il ne sera peut-être pas inutile de montrer par un exemple comment ces réductions s'effectuent dans les cas particuliers.

Soit proposée l'équation $333y^2-719yz+388z^2=H$; pour avoir par une opération uniforme la transformée du premier membre, je développe en fraction continue une racine de l'équation $333x^2-719x+388=0$, et je calcule en même temps les fractions convergentes qui en résultent. Voici le détail de l'opération qu'il suffit de continuer jusqu'à ce que les quotiens-complets cessent d'être irréguliers; mais on l'a prolongée pendant une période entière, parce que cette période n'est composée que de trois termes :

$$x = \frac{719+\sqrt{145}}{666} = 1 +$$

$$\frac{-53+\sqrt{145}}{-4} = 10 +$$

$$\frac{13+\sqrt{145}}{6} = 4 +$$

$$* \quad \frac{11+\sqrt{145}}{4} = 5 +$$

$$\frac{9+\sqrt{145}}{16} = 1 +$$

$$\frac{7+\sqrt{145}}{6} = 3 +$$

$$* \quad \frac{11+\sqrt{145}}{4} = 5 +$$

| | |
|---|---|
| 1 : | 0 |
| 1 : | 1 |
| 11 : | 10 |
| 45 : | 41 |
| &c. | |

De-là, et des articles 91 et 95, on conclut que si l'on fait

$$y = 45y' + 11z'$$
$$z = 41y' + 10z',$$

on aura pour transformée du premier membre :

$$-(2y'y' - 11y'z' - 3z'z').$$

Ce résultat trouvé *a priori* est d'autant plus remarquable, qu'il seroit assez long de le vérifier directement par la substitution des valeurs de $y$ et de $z$ ; on le vérifieroit plus promptement, en y substituant les valeurs de $y'$ et de $z'$, savoir $y' = 11z - 10y$, $z' = 41y - 45z$, ce qui reproduiroit la formule proposée.

Au reste, la transformée $-2y'y' + 11y'z' + 3z'z'$ n'est pas encore réduite à la forme convenable, et pour faire en sorte que le coefficient moyen ne soit pas plus grand que les extrêmes, il faut prendre $y' = u' + 3z'$; ce qui donnera $-2u'^2 - u'z' + 18z'^2$; donc il faut faire

$$y = 45u' + 146z'$$
$$z = 41u' + 133z',$$

et la transformée de l'équation proposée, réduite à la forme la plus simple, sera

$$2u'u' + u'z' - 18z'^2 = -H.$$

## §. XIV. *Développement en fraction continue des racines des équations d'un degré quelconque.*

(96) Soit proposé de développer en fraction continue une racine réelle de l'équation

$$ax^n+bx^{n-1}+cx^{n-2}+\ldots\ldots+k=0,$$

dont les coefficiens sont des nombres entiers positifs ou négatifs. D'abord on peut supposer que cette équation n'est divisible par aucun facteur rationnel, car autrement on pourroit supprimer le facteur étranger à la racine qu'on veut développer, et l'opération en deviendroit beaucoup plus simple : par la même raison, l'équation proposée ne pourra avoir des racines égales, car si elle en avoit, elle seroit divisible par un facteur rationnel qu'on trouveroit aisément par les méthodes connues.

Cela posé, la racine dont il s'agit, étant choisie entre toutes les autres sera connue à moins d'une unité près. Soit $\alpha$ le plus petit des deux entiers prochains entre lesquels elle est contenue, on fera, si $x$ est positif, $x=\alpha+\frac{1}{x'}$, ou s'il est négatif $x=-\alpha-\frac{1}{x'}$, et on sera sûr que la valeur de $x'$ est positive et plus grande que l'unité. Substituant cette valeur dans l'équation proposée, on aura la transformée

$$a'x'^n+b'x'^{n-1}+c'x'^{n-2}\ldots\ldots+k'=0,$$

qui servira à déterminer $x'$. Or on sait déjà que la valeur de $x'$ dont on a besoin, est positive et plus grande que l'unité ; il peut même y avoir plusieurs valeurs de $x'$ qui remplissent ces deux conditions, parce qu'il peut y avoir plusieurs racines de l'équation proposée qui, sans être égales, soient comprises entre $\alpha$ et $\alpha+1$. On essaiera donc pour $x'$ les nombres successifs 1, 2, 3, &c. jusqu'à ce que, par les caractères connus, on trouve les nombres entiers les plus proches entre lesquels tombe la valeur de $x'$. Soit $\mathcal{C}$ le plus petit des deux, on fera $x'=\mathcal{C}+\frac{1}{x''}$, et en substituant cette valeur, on

aura, pour déterminer $x''$, une nouvelle transformée

$$a''x''^{n}+b''x''^{n-1}+\dots+k''=0,$$

qu'on traitera comme la précédente. En continuant ainsi aussi loin qu'on voudra, il est clair que la valeur de $x$ sera exprimée par cette fraction continue

$$x=\alpha+\cfrac{1}{\beta+\cfrac{1}{\gamma+\ \&c.}}$$

Et au moyen de ces quotiens connus, on calculera à l'ordinaire les fractions convergentes vers $x$.

(99) Soient $\frac{p^\circ}{q^\circ}$, $\frac{p}{q}$, deux de ces fractions conséculives et $z$ le quotient-complet qui répond à la dernière, on aura par la propriété connue $x=\frac{pz+p^\circ}{qz+q^\circ}$; donc on peut trouver directement une transformée quelconque, en substituant cette valeur au lieu de $x$ dans l'équation proposée. Soit cette transformée

$$Az^{n}+Bz^{n-1}+Cz^{n-2}\dots+K=0,$$

et on aura par conséquent

$$A=ap^{n}+bp^{n-1}q+cp^{n-2}q^{2}\dots+kq^{n}$$
$$K=ap^{\circ n}+bp^{\circ n-1}q^{\circ}+cp^{\circ n-2}q^{\circ 2}\dots+kq^{\circ n}.$$

De sorte que suivant nos notations ordinaires, on auroit en général $K=A^{\circ}$, ou $K'=A$. Mais il est beaucoup plus simple de déduire successivement chaque transformée de la transformée précédente, comme on l'a déjà expliqué. Pour rendre à cet égard le calcul aussi simple qu'il est possible, observons qu'en faisant $z=\mu+\frac{1}{z'}$, l'équation précédente en $z$ devenant

$$A'z'^{n}+B'z'^{n-1}+C'z'^{n-2}\dots+K'=0,$$

on auroit

$$A'=A\mu^{n}+B\mu^{n-1}+C\mu^{n-2}\dots+K$$
$$B'=nA\mu^{n-1}+(n-1)B\mu^{n-2}+(n-2)C\mu^{n-3}+\&c,$$
$$C'=\frac{n.n-1}{2}A\mu^{n-2}+\frac{n-1.n-2}{2}B\mu^{n-3}+\&c.$$
$$\vdots$$
$$K'=A$$

Donc si la fonction $Az^n+Bz^{n-1}+Cz^{n-2}\ldots+K$ est désignée par $\varphi : z$ ou $\varphi$, et qu'on forme successivement par la différentiation les quantités $\varphi$, $\frac{d\varphi}{dz}$, $\frac{dd\varphi}{2dz^2}$, $\frac{d^3\varphi}{2.3dz^3}$, &c., qu'ensuite on substitue au lieu de $z$ sa valeur approchée $\mu$, ces quantités deviendront respectivement les valeurs des coefficiens $A'$, $B'$, $C'$, &c. de la transformée suivante.

Telle est la méthode que Lagrange a le premier proposée pour le développement des racines des équations en fraction continue; mais cette méthode seroit d'une longueur rebutante dans la pratique, si le même auteur n'eût indiqué un moyen fort simple de continuer sans tâtonnement la suite des entiers $\alpha$, $\beta$, $\gamma$, $\delta$, &c. lorsque quelques-uns des premiers termes sont déjà connus. Voici en quoi consiste ce perfectionnement.

(100) La formule $x=\frac{pz+p^\circ}{qz+q^\circ}$, donne $z=\frac{q^\circ x-p^\circ}{p-qx}$, ou

$$z+\frac{q^\circ}{q}=\frac{pq^\circ-p^\circ q}{q(p-qx)}.$$

$x$ désignant toujours la racine qu'on veut développer, soient $x_1$, $x_2$, $x_3$, &c. les autres racines de la proposée, et soient $z_1$, $z_2$, $z_3$, &c. les valeurs correspondantes de $z$; alors, outre l'équation précédente, on aura les $n-1$ équations qui suivent:

$$z_1+\frac{q^\circ}{q}=\frac{pq^\circ-p^\circ q}{q(p-qx_1)}$$
$$z_2+\frac{q^\circ}{q}=\frac{pq^\circ-p^\circ q}{q(p-qx_2)}$$
$$z_3+\frac{q^\circ}{q}=\frac{pq^\circ-p^\circ q}{q(p-qx_3)}$$
&c.

Ajoutons toutes ces équations, et observons que l'équation en $z$ étant $Az^n+Bz^{n-1}+$ &c. $=0$, on a $z+z_1+z_2+z_3+$ &c. $=-\frac{B}{A}$, la somme sera

$$-z-\frac{B}{A}+(n-1)\frac{q^\circ}{q}=(pq^\circ-p^\circ q)\frac{\Delta}{q^2}=\pm\frac{\Delta}{q^2}$$

où l'on a fait pour abréger :

$$\Delta = \frac{1}{\frac{p}{q} - x_1} + \frac{1}{\frac{p}{q} - x_2} + \frac{1}{\frac{p}{q} - x_3} + \&c.$$

Maintenant si la quantité $\frac{\Delta}{q^2}$ est assez petite pour pouvoir être négligée, il est clair que la valeur de $z$ sera donnée d'une manière directe et exempte de tâtonnement, par la formule

$$z = (n-1)\frac{q^{\circ}}{q} - \frac{B}{A}.$$

Il faudra donc preudre pour $\mu$ l'eutier le plus grand, contenu dans cette valeur, et cet entier $\mu$ sera le quotient qui répond à la fraction convergente $\frac{p}{q}$. Au moyen de ce quotient on calculera la fraction suivante $\frac{p'}{q'}$, et la transformée suivante en $z'$; de sorte que l'opération pourra être continuée aussi loin qu'on voudra, sans aucun tâtonnement.

(101) La quantité $\Delta$ varie suivant les différentes fractions $\frac{p}{q}$ auxquelles elle se rapporte; elle ne peut devenir infinie, parce qu'il faudroit pour cela qu'un dénominateur tel que $\frac{p}{q} - x_1$, fût zéro, et par conséquent que l'équation proposée eût un diviseur rationnel $p - qx$, ce qui est contre la supposition.

Néanmoins cette quantité $\Delta$ pourra quelquefois être un nombre assez considérable, et cela aura lieu, s'il y a peu de différence entre la racine $x$ et une ou plusieurs des autres racines $x_1$, $x_2$, &c. Au reste, comme les fractions convergentes $\frac{p}{q}$ approchent rapidement de la valeur de $x$, il est clair que les quantités $\Delta$ s'approcheront non moins rapidement de la limite

$$T = \frac{1}{x - x_1} + \frac{1}{x - x_2} + \frac{1}{x - x_3} + \&c.$$

Donc si on continue par la première méthode, le calcul des termes de la fraction continue et celui des fractions convergentes, jusqu'à ce que $\frac{T}{q^2}$ soit plus petit qu'une fraction déterminée $\frac{1}{m}$, ou qu'on

ait

soit $q > \sqrt{Tm}$ ($T$ étant pris positivement), il est clair que la valeur de $x$ trouvée ci-dessus, savoir :

$$x = (n-1)\frac{q'}{q} - \frac{B}{A}$$

ne sera en erreur que d'une quantité moindre que $\frac{1}{m}$.

Donc une connoissance assez imparfaite des racines de l'équation proposée, et seulement de celles qui sont très-peu différentes de la racine qu'on développe, suffit pour déterminer la limite après laquelle on peut continuer l'opération sans aucun tâtonnement, par le moyen de la formule précédente.

Parmi ces racines, peu différentes de la racine donnée, il faut comprendre même les racines imaginaires ; car *analytiquement parlant*, une racine $\alpha + \mathcal{C}\sqrt{-1}$ dans laquelle $\frac{\mathcal{C}}{\alpha}$ est très-petit, est censée peu différente de $\alpha$. Si donc on a une racine imaginaire $x_1 = \alpha + \mathcal{C}\sqrt{-1}$, et par conséquent une autre $x_2 = \alpha - \mathcal{C}\sqrt{-1}$, il résultera de ces deux racines substituées dans la valeur de $T$ les deux termes

$$\frac{1}{x-\alpha-\mathcal{C}\sqrt{-1}} + \frac{1}{x-\alpha+\mathcal{C}\sqrt{-1}};$$

lesquelles se réduisent à la quantité réelle $\frac{2(x-\alpha)}{(x-\alpha)^2+\mathcal{C}^2}$. Cette quantité ne peut excéder le *maximum* $\frac{1}{\mathcal{C}}$, cependant elle peut être encore assez grande lorsque $\mathcal{C}$ est très-petit, ainsi que $x - \alpha$.

Si la différence de la racine $x$ avec chacune des autres racines (différence qui se convertit en somme lorsque les deux racines sont de signes contraires) est plus grande que l'unité, alors il est clair que $T$ sera moindre que $n-1$, et la limite de $q$ sera $q > \sqrt{(n-1)m}$. Valeur, comme on voit, assez petite ; de sorte qu'on pourra employer la formule presque dès le commencement de l'opération, et alors il n'y aura presqu'aucun tâtonnement.

Si au contraire la racine $x$ diffère très-peu d'une ou de plusieurs racines réelles ou imaginaires de l'équation proposée, alors la première méthode doit être employée dans un certain nombre de termes ; mais on ne tardera pas à atteindre la limite $q > \sqrt{Tm}$, après quoi

l'opération se continuera sans le moindre tâtonnement. Au reste, on peut observer que s'il y a réellement deux ou plusieurs racines peu différentes entr'elles, l'équation

$$nax^{n-1} + (n-1)bx^{n-2} + (n-2)cx^{n-3} + \&c. = 0$$

qui est vraie, lorsqu'il y a des racines égales, aura lieu d'une manière approchée lorsqu'il y a des racines peu inégales. On pourra donc *assez souvent*, en combinant cette équation avec la proposée, en déduire une valeur approchée de ces racines peu différentes entr'elles; de sorte qu'alors on évitera encore presque tout tâtonnement. Nous ne donnons cependant pas ce moyen comme absolument général, parce que la combinaison de l'équation proposée avec cette équation secondaire, peut multiplier l'erreur attachée à celle-ci, et empêcher le résultat d'être suffisamment exact.

(102) Lorsque l'opération du développement est avancée jusqu'à un certain point, et que les dénominateurs $q$ des fractions convergentes commencent à être un peu grands, la formule $z = (n-1)\frac{q^{\circ}}{q} - \frac{B}{A}$ donne non-seulement le quotient $\mu$ correspondant à la fraction $\frac{p}{q}$; mais en développant cette valeur de $z$ en fraction continue, les quotiens qu'on obtient de ce développement peuvent être employés à la suite des quotiens déjà trouvés, et sont exacts jusqu'à une limite que nous allons déterminer.

La valeur exacte de $z$ étant

$$z = (n-1)\frac{q^{\circ}}{q} - \frac{B}{A} \pm \frac{\Delta}{q^{2}},$$

le terme négligé $\frac{\Delta}{q^{2}}$ occasionne dans $x$ une erreur qui sera donnée par l'équation rigoureuse $p - qx = \frac{\pm 1}{qz + q^{\circ}}$, en mettant $z \pm \frac{\Delta}{q^{2}}$ à la place de $z$, et $x + \delta x$ à la place de $x$. De cette manière, on trouve

$$\delta x = \frac{\Delta}{q^{2}(qz+q^{\circ})^{2}}.$$

Soient donc $\mu, \mu', \mu'', \ldots \omega$ les quotiens qui résultent du développement de la quantité $(n-1)\frac{q^{\circ}}{q} - \frac{B}{A}$, et supposons qu'en

continuant par le moyen de ces quotiens le calcul des fractions convergentes vers $x$, on parvienne à la fraction $\frac{P}{Q}$, cette dernière sera encore (n°. 9) une fraction convergente, si l'on a $\frac{P}{Q}-x<\frac{1}{2Q^2}$; donc tant que $\frac{1}{Q^2}$ sera $>\frac{2\Delta}{q^2(qz+q^\circ)^2}$, ou tant qu'on aura $Q<\frac{q(qz+q^\circ)}{\sqrt{2\Delta}}$, ou à-peu-près $Q<\frac{q^2\mu}{\sqrt{2T}}$, la fraction $\frac{P}{Q}$ sera encore l'une des fractions convergentes vers $x$. D'où il suit qu'à partir de la fraction convergente $\frac{p}{q}$, la valeur de $z$ correspondante, développée en fraction continue, fournit les quotiens nécessaires pour prolonger les fractions convergentes vers $x$, jusqu'à ce qu'elles aient environ deux fois autant de chiffres que celle d'où l'on est parti.

### EXEMPLE I.

(103) Soit proposée l'équation $x^3-x^2-2x+1=0$, dont on sait que les racines sont $x=2\cos\frac{1}{7}\pi$, $x=-2\cos\frac{2}{7}\pi$, $x=2\cos\frac{3}{7}\pi$, $\pi$ étant la demi-circonférence dont le rayon est 1. On aura donc à-peu-près $x=1,802$; $x=-1,247$; $x=0,445$. Pour développer d'abord la première racine, on observera que les différences de cette racine avec les deux autres étant $x-x1=3,049$; $x-x2=1,357$, on a la limite $T=\frac{1}{3,049}+\frac{1}{1,357}=1$ à-peu-près; et ainsi la formule qui donne la valeur de $z$ sera exacte à moins de $\frac{1}{10}$ lorsqu'on aura $q>\sqrt{10}$ ou $q>3$, et à moins de $\frac{1}{100}$ lorsqu'on aura $q>10$. Il n'y aura donc dans ce cas aucun tâtonnement. Voici au reste les détails de l'opération.

La valeur de $x$ qu'on veut développer étant comprise entre 1 et 2, je fais $x=1+\frac{1}{z}$, et j'ai la transformée

$$-z^3-z^2+2z+1=0.$$

Dans celle-ci il est aisé de voir que la valeur positive de $z$ est encore comprise entre 1 et 2, ainsi on fera $z=1+\frac{1}{z'}$, ou simple-

S 2

ment on mettra $1+\frac{1}{z}$ à la place de $z$; car il est inutile de distinguer par des accens les inconnues des transformées successives, et on sait bien qu'elles doivent être différentes. La transformée sera donc

$$z^3-3z^2-4z-1=0.$$

Dans cette dernière, la valeur de $z$ est comprise entre 4 et 5, de sorte qu'il faut mettre $4+\frac{1}{z}$ à la place de $z$. Mais pour faire cette substitution suivant la méthode qui a été indiquée (n°. 99), je forme successivement les quantités

$$\varphi = z^3-3z^2-4z-1$$
$$\frac{d\varphi}{dz}=3z^2-6z-4$$
$$\frac{dd\varphi}{2dz^2}=3z-3$$
$$\frac{d^3\varphi}{2.3dz^3}=1.$$

Je substitue ensuite dans ces quantités la valeur $z=4$, et j'ai les quatre nombres $-1$, 20, 9, 1, d'où résulte la transformée suivante:

$$-z^3+20z^2+9z+1=0.$$

Maintenant l'opération est plus avancée qu'il ne faut pour être continuée sans tâtonnement; et d'abord au moyen des quotiens trouvés 1, 1, 4, je forme les fractions convergentes comme il suit:

| | | | | |
|---|---|---|---|---|
| Quotiens ..... | 1, | 1, | 4 | |
| Fract. converg. | $\frac{1}{0}$, | $\frac{1}{1}$, | $\frac{2}{1}$, | $\frac{9}{5}$ |

Et la quantité $z$ déterminée par la dernière transformée sera le quotient-complet qui répond à la fraction $\frac{9}{5}$. Mais en vertu de la formule $z=\frac{2q^\circ}{q}-\frac{B}{A}$, on a $z=\frac{2}{5}+20$, donc 20 est l'entier compris dans $z$. Au moyen de ce nouveau quotient 20, on avancera d'un terme le calcul des fractions convergentes, savoir:

$$1,\quad 1,\quad 4,\quad 20$$
$$\frac{1}{0},\ \frac{1}{1},\ \frac{2}{1},\ \frac{9}{5},\ \frac{182}{101}.$$

Et pour avoir la transformée suivante, on formera les quatre quantités

$$\varphi = -z^3 + 20z^2 + 9z + 1$$

$$\frac{d\varphi}{dz} = -3z^2 + 40z + 9$$

$$\frac{dd\varphi}{2dz^2} = -3z + 20$$

$$\frac{d^3\varphi}{2.3dz^3} = -1,$$

on y substituera la valeur $z = 20$, ce qui donnera les quatre nombres 181, −391, −40, −1; partant la nouvelle transformée sera

$$181\,z^3 - 391\,z^2 - 40\,z - 1 = 0.$$

La valeur approchée de $z$ dans cette transformée sera, suivant la formule, $z = \frac{10}{101} + \frac{391}{181} = 2 +$, de sorte que 2 est le quotient suivant. En procédant ainsi, on trouvera les résultats consignés dans le tableau suivant.

*Développement de la racine comprise entre* 1 *et* 2.

| Équation proposée, et ses transformées successives. | Racine approchée. | Fractions convergentes. |
|---|---|---|
| $x^3 - x^2 - 2x + 1 = 0$ | 1 | 1 : 0 |
| $-z^3 - z^2 + 2z + 1 = 0$ | 1 | 1 : 1 |
| $z^3 - 3z^2 - 4z - 1 = 0$ | 4 | 2 : 1 |
| $-z^3 + 20z^2 + 9z + 1 = 0$ | 20 | 9 : 5 |
| $181z^3 - 391z^2 - 40z - 1 = 0$ | 2 | 182 : 101 |
| $-197z^3 + 568z^2 + 695z + 181 = 0$ | 3 | 373 : 207 |
| $2059z^3 - 1216z^2 - 1205z - 197 = 0$ | 1 | 1301 : 722 |
| $-559z^3 + 2540z^2 + 4961z + 2059 = 0$ | 6 | 1674 : 929 |
| $2521z^3 - 24931z^2 - 7522z - 559 = 0$ | 10 | 11345 : 6296 |
| $-47879z^3 + 250158z^2 + 50699z + 2521 = 0$ | | 115124 : 63889 |
| &c. | | &c. |

La dernière transformée a pour racine approchée

$$z = \frac{12592}{63889} + \frac{250158}{47879};$$

quantité qui étant réduite en une seule fraction, et développée en fraction continue, donne les quotiens 5, 2, 2, 1, 2, 2, 1, 18, 1, 1, 3, &c. On pourra donc, au moyen de ces quotiens mis à la suite des quotiens déjà trouvés, continuer le calcul des fractions convergentes, jusqu'à ce que leurs termes aient 11 ou 12 chiffres. Par des opérations semblables, on développera les deux autres racines, comme on le voit dans les tableaux suivans :

*Développement de la racine comprise entre* 0 *et* 1.

| Équation proposée et ses transformées. | Racine approchée. | Fractions convergentes. |
|---|---|---|
| $x^3 - x^2 - 2x + 1 = 0$ | 0 | 1 : 0 |
| $z^3 - 2z^2 - z + 1 = 0$ | 2 | 0 : 1 |
| $-z^3 + 3z^2 + 4z + 1 = 0$ | 4 | 1 : 2 |
| $z^3 - 20z^2 - 9z - 1 = 0$ | 20 | 4 : 9 |
| | 2 | 81 : 182 |
| Suivent les mêmes trans- | 3 | 166 : 373 |
| formées, et par conséquent les | 1 | 579 : 1301 |
| mêmes quotiens que dans le | 6 | 745 : 1674 |
| développement de la première | 10 | 5049 : 11345 |
| racine. | 5 | 51235 : 115124 |
| | 2 | 261224 : 586965 |
| | &c. | &c. |

*Développement de la racine comprise entre* −1 *et* −2.

| Équation proposée et ses transformées. | Racine approchée. | Fractions convergentes. |
|---|---|---|
| $x^3 - x^2 - 2x + 1 = 0$ | −1 | −1 : 0 |
| $z^3 - 3z^2 - 4z - 1 = 0$ | 4 | −1 : 1 |
| $-z^3 + 20z^2 + 9z + 1 = 0$ | 20 | −5 : 4 |
| | 2 | −101 : 81 |
| Suivent encore les mêmes | 3 | −207 : 166 |
| transformées et les mêmes | 1 | −722 : 579 |
| quotiens qu'on a trouvés dans | 6 | −929 : 745 |
| le développement de la pre- | 10 | −6296 : 5049 |
| mière racine. | 5 | −63889 : 51235 |
| | &c. | &c. |

(104) Dans cet exemple, il est très-remarquable qu'on trouve un rapport entre les trois racines, au moyen duquel le développement de la première racine suffit pour donner celui des deux autres. Ce rapport est tel, que si on appelle $\zeta$ une même racine de l'équation $z^3 - 3z^2 - 4z - 1 = 0$, celle par exemple qui est entre 4 et 5, les trois racines de la proposée seront :

$$x = 1 + \cfrac{1}{1 + \cfrac{1}{\zeta}} = \frac{2\zeta + 1}{1 + \zeta}$$

$$x_1 = \cfrac{1}{2 + \cfrac{1}{\zeta}} = \frac{\zeta}{2\zeta + 1}$$

$$x_2 = -1 - \frac{1}{\zeta} = -\left(\frac{1 + \zeta}{\zeta}\right);$$

ou si on appelle $\alpha$ la première valeur de $x$, les deux autres seront :

$$x_1 = \cfrac{1}{1 + \cfrac{1}{\alpha - 1}} = \frac{\alpha - 1}{\alpha}$$

$$x_2 = -\frac{1}{\alpha - 1}.$$

Ces propriétés se vérifieroient aisément par les formules des sinus, puisqu'on a $x = 2\cos\frac{1}{7}\pi$, $x_1 = 2\cos\frac{3}{7}\pi$, $x_2 = 2\cos\frac{5}{7}\pi = -2\cos\frac{2}{7}\pi$. Nous remarquerons au reste que l'équation dont il s'agit tire son origine de l'équation $r^7 - 1 = 0$, où l'on a fait $r^2 + rx + 1 = 0$; elle serviroit aussi à inscrire le polygone régulier de 7 et celui de 14 côtés, car on a le côté de l'heptagone régulier $= 2\sin\frac{1}{7}\pi = \sqrt{(4 - x^2)}$ $= \frac{2}{\sqrt{7}}(x + 2)(x - \frac{1}{2})$, et celui du polygone de 14 côtés $= 2\cos\frac{3}{7}\pi = x_1$.

Toutes les équations relatives à la division du cercle sont telles, qu'une de leurs racines suffit pour déterminer rationnellement toutes les autres; mais il en existe une infinité d'autres qui offrent la même facilité, et entre toutes ces équations, on doit distinguer sur-tout celles dont une racine développée en fraction continue suffit pour donner le développement de toutes les autres racines. Cet objet paroît mériter l'attention des Analystes, et il pourroit fournir des résultats intéressans.

EXEMPLE II.

(105) Soit proposée l'équation $x^3+11x^2-102x+181=0$, dont les racines approchées sont $x=3,2131$; $x=3,2295$; $x=-17,442$.

Puisqu'il y a deux racines très-peu inégales, on pourroit les trouver directement, en combinant l'équation proposée avec l'équation des racines égales $3x^2+22x-102=0$. Or celle-ci donne en effet $x=3,22$ à-peu-près, valeur qui étant développée donne les premiers quotiens 3, 4, 1, au moyen desquels on pourra commencer l'opération dont voici le détail :

| $x^3+11x^2-102x+181=0$ | 3 | 1 : 0 |
|---|---|---|
| $z^3-9z^2+20z+1=0$ | 4 | 3 : 1 |
| $z^3-4z^2+3z+1=0$ | 1 | 13 : 4 |
| $z^3-2z^2-z+1=0$ | 2 | 16 : 5 |
| $-z^3+3z^2+4z+1=0$ | 4 | 45 : 14 |
| Sans aller plus loin, on voit | 20 | 196 : 61 |
| que les transformées et les quo- | 2 | 3965 : 1234 |
| tiens ultérieurs seront comme | 3 | 8126 : 2529 |
| dans l'exemple précédent. | 1 | 28343 : 8821 |
| | &c. | &c. |

Les rapports qu'on observe entre les résultats de ces deux exemples, sont fondés sur ce qu'en faisant dans ce dernier $x=\frac{13z+16}{4z+5}$, on a pour transformée $z^3-z^2-2z+1=0$, qui est l'équation de l'exemple I.

EXEMPLE III.

(106) L'équation $x^4-x^3-3x^2+2x+1=0$ auroit pour racines $x=2\cos\frac{\pi}{9}$, $x=-2\cos\frac{2\pi}{9}$, $x=2\cos\frac{3\pi}{9}$, $x=-2\cos\frac{4\pi}{9}$ : mais en excluant la racine $2\cos\frac{3\pi}{9}$ qui se réduit à l'unité, on a l'équation $x^3-3x-1=0$ dont les racines sont $x=2\cos\frac{\pi}{9}$, $x=-2\cos\frac{2\pi}{9}$ : $x=-2\cos\frac{4\pi}{9}$. Voici le développement de la plus petite $-2\cos\frac{4\pi}{9}$.

$x^3-3x-1=0$

| $x^3-3x-1=0$ | $-0$ | $-1:0$ |
|---|---|---|
| $-z^3+3z^2-1=0$ | 2 | $-0:1$ |
| $3z^3-3z-1=0$ | 1 | $-1:2$ |
| $-z^3+6z^2+9z+3=0$ | 7 | $-1:3$ |
| $17z^3-54z^2-15z-1=0$ | 3 | $-8:23$ |
| $-73z^3+120z^2+99z+17=0$ | 2 | $-25:72$ |
| $111z^3-297z^2-318z-73=0$ | 3 | $-58:167$ |
| $-703z^3+897z^2+702z+111=0$ | 1 | $-199:573$ |
| $1007z^3+387z^2-1212z-703=0$ | 1 | $-257:740$ |
| $-521z^3+2583z^2+3408z+1007=0$ | 6 | $-456:1313$ |
| $1907z^3-21864z^2-6790z-521=0$ | 11 | $-2993:8618$ |
| &c. | &c. | &c. |

La dernière transformée aura pour racine approchée

$$\frac{1313}{4309}+\frac{21864}{1907}=11\,\frac{6325974}{8217263},$$

et le développement de cette fraction donnera à la suite de 11 les quotiens 1, 3, 2, 1, 9, 1, 2, 5, &c., au moyen desquels l'approximation des fractions convergentes peut être poussée jusqu'à ce que les dénominateurs n'excèdent pas $(8618)^2$.

*Développement de la racine* $x=2\cos\frac{\pi}{9}$.

| $x^3-3x-1=0$ | 1 | $1:0$ |
|---|---|---|
| $-3z^3+3z+1=0$ | 1 | $1:1$ |
| $z^3-6z^2-9z-3=0$ | 7 | $2:1$ |
| $-17z^3+54z^2+15z+1=0$ | 3 | $15:8$ |
| | 2 | $47:25$ |
| Les autres transformées sont | 3 | $109:58$ |
| les mêmes que dans le déve- | 1 | $374:199$ |
| loppement de la première ra- | 1 | $483:257$ |
| cine. | 6 | $857:456$ |
| | 11 | $5625:2993$ |
| | &c. | &c. |

*Développement de la racine* $x = -2\cos\frac{2\pi}{9}$.

| $x^3 - 3x - 1 = 0$ | $-1$ | $-1 : 0$ |
|---|---|---|
| $z^3 - 3z - 1 = 0$ | 1 | $-1 : 1$ |
| $-3z^3 + 3z + 1 = 0$ | 1 | $-2 : 1$ |
| $z^3 - 6z^2 - 9z - 3 = 0$ | 7 | $-3 : 2$ |
| | 3 | $-23 : 15$ |
| Les autres transformées | 2 | $-72 : 47$ |
| comme dans la racine précé- | 3 | $-167 : 109$ |
| dente. | 1 | $-573 : 374$ |
| | 1 | $-740 : 483$ |
| | 6 | $-1313 : 857$ |
| | 11 | $-8618 : 5625$ |
| | &c. | &c. |

Ces rapports entre les racines pourront se vérifier aisément par les formules connues des sinus.

(107) Nous avons déjà remarqué (n°. 99), que si l'équation proposée est

$$ax^n + bx^{n-1} + cx^{n-2} \ldots\ldots + k = 0,$$

et qu'une de ses transformées, correspondante à la fraction convergente $\frac{p}{q}$, soit

$$\mathcal{A}z^n + Bz^{n-1} + Cz^{n-2} \ldots\ldots + K = 0,$$

on aura

$$\mathcal{A} = ap^n + bp^{n-1}q + cp^{n-2}q^2 \ldots\ldots + kq^n.$$

De-là il suit que si on a à résoudre l'équation indéterminée

$$at^n + bt^{n-1}u + ct^{n-2}u^2 \ldots\ldots + ku^n = \mathcal{A};$$

et que le nombre $\mathcal{A}$ se trouve coefficient du premier terme de l'une des transformées successives données par le développement de $x$ en fraction continue, la fraction correspondante $\frac{p}{q}$ sera une valeur de $\frac{t}{u}$ et donnera une solution de l'équation proposée. On aura donc ainsi autant de ces solutions particulières qu'on trouvera de fois le nombre $\mathcal{A}$ parmi les coefficiens dont il s'agit; mais il faudra en

outre que le signe de ce coefficient, tel qu'il est donné par la série des opérations, s'accorde avec celui de $A$ dans le second membre de l'équation proposée.

Pour passer de l'équation proposée à sa transformée en $z$, on peut faire directement $x = \frac{pz+p^\circ}{qz+q^\circ}$; réciproquement pour revenir de la transformée à la proposée, il faut faire $z = \frac{q^\circ x - p^\circ}{p - qx}$; ce qui donnera

$$\pm a = A(-q^\circ)^n + B(-q^\circ)^{n-1}q + C(-q^\circ)^{n-2}q^2 \ldots\ldots + Kq^n;$$

de sorte que si on avoit à résoudre l'équation indéterminée

$$a = Ay^n + By^{n-1}u + Cy^{n-2}u^2 + \ldots\ldots + Ku^n,$$

on y satisferoit en prenant $\frac{y}{u} = \frac{-q^\circ}{q}$. Et le rapport que nous établissons ici entre l'équation proposée et chacune de ses transformées, a également lieu entre deux transformées quelconques, pourvu que les fractions convergentes soient calculées d'après les quotiens intermédiaires.

Ainsi dans l'exemple premier, on peut comparer directement la seconde transformée $x^3 - 3x^2 - 4x - 1 = 0$ à la neuvième $-47879z^3 + 250158z^2 + 50699z + 2521 = 0$; mais pour cela, il faut calculer les fractions convergentes vers une racine de l'équation $x^3 - 3x^2 - 4x - 1 = 0$, ce qui se fera au moyen des quotiens trouvés 4, 20, 2, 3, 1, 6, 10; voici ce calcul:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Quotiens..... | | 4, | 20, | 2, | 3, | 1, | 6, | 10 |
| Fract. converg. | $\frac{1}{0}$, | $\frac{4}{1}$, | $\frac{81}{20}$, | $\frac{166}{41}$, | $\frac{579}{143}$, | $\frac{745}{184}$, | $\frac{5049}{1247}$, | $\frac{51235}{12654}$. |

On aura donc $x = \frac{51235z + 5049}{12654z + 1247}$, ou $z = \frac{-1247x + 5049}{12654x - 51235}$.

On voit en même temps que si on avoit à resoudre l'équation

$$47879t^3 + 250158t^2u - 50699tu^2 + 2521u^3 = 1,$$

on y satisferoit en faisant $t = 1247$, $u = 12654$.

Une telle réduction entre de si grands nombres paroît remarquable; cependant pour peu qu'on y réfléchisse, on verra que toutes les transformées comprises dans le développement de la même racine

jouissent de la même propriété, c'est-à-dire que si l'une quelconque de ces transformées est représentée par $\mathcal{A}z^3+Bz^2+Cz+D=0$, les nombres $\mathcal{A}$, $B$, $C$, $D$ pouvant s'élever à une grandeur quelconque, on satisfera toujours à l'équation

$$\mathcal{A}t^3+Bt^2u+Ctu^2+Du^3=1,$$

en prenant $t=-q^2, u=q$, $\frac{p}{q}$ étant la fraction convergente à laquelle répond le quotient-complet $z$.

Si l'on considère de plus que la proposée $x^3-x^2-2x+1=0$ et ses trois premières transformées ont à leur premier terme l'unité pour coefficient, et que chacune de ces quatre équations peut être regardée comme l'équation principale qui, par le développement de sa racine, fournit toutes les autres transformées, on en conclura qu'il y a toujours au moins quatre manières de réduire à l'unité la quantité $\mathcal{A}t^3+Bt^2u+Ctu^2+Du^3$. Par exemple, si l'on se propose encore l'équation

$$47879t^3+250158t^2u-50699tu^2+2521u^3=1,$$

on y satisfera de ces quatre manières :

$$\begin{array}{ll} t=6296 & u=63889 \\ t=5049 & u=51235 \\ t=1247 & u=12654 \\ t=\phantom{00}61 & u=\phantom{0}619. \end{array}$$

(108) Mais on peut encore trouver d'autres solutions par le développement des deux autres racines de la même équation. En effet, puisqu'en partant de l'équation

$$47879z^3+250158z^2-50699z+2521=0,$$

et faisant $z=\frac{6296x-11345}{63889x-115124}$, on a la transformée

$$x^3-x^2-2x+1=0,$$

on peut supposer qu'on est parvenu à ce résultat, en développant en fraction continue une racine de l'équation en $z$, comprise entre 0 et 1. Voici l'opération qui seroit l'inverse de celle de l'exemple I :

| | | |
|---|---|---|
| $o = 47879 z^3 + 250158 z^2 - 50699 z + 2521$ | 0 | 1 : 0 |
| $o = 2521 y^3 - 50699 y^2 + 250158 y + 47879$ | 10 | 0 : 1 |
| $o = 559 y^3 - 7522 y^2 + 24931 y + 2521$ | 6 | 1 : 10 |
| $o = 2059 y^3 - 1961 y^2 + 2540 y + 559$ | 1 | 6 : 61 |
| $o = 197 y^3 - 1205 y^2 + 1216 y + 2059$ | 3 | 7 : 71 |
| $o = 181 y^3 - 695 y^2 + 568 y + 197$ | 2 | 27 : 274 |
| $o = y^3 - 40 y^2 + 391 y + 181$ | 20 | 61 : 619 |
| $o = y^3 - 9 y^2 + 20 y + 1$ | 4 | 1247 : 12654 |
| $o = y^3 - 4 y^2 + 3 y + 1$ | 1 | 5049 : 51235 |
| * $o = y^3 - 2 y^2 - y + 1$ | 1* | 6296 : 63889 |
| $o = -Z^3 - 2Z^2 + Z + 1$ | | 11345 : 115124 |

Arrivé à cette transformée, on auroit $z = \frac{11345 Z + 6296}{115124 Z + 63889}$; ainsi en mettant $-\frac{1}{x}$ à la place de $Z$, on voit que la substitution de la valeur $z = \frac{6296 x - 11345}{63889 x - 115124}$ donne en effet la transformée $x^3 - x^2 - 2x + 1 = o$. Mais le développement précédent, qui est exact jusques dans l'avant-dernière transformée, cesse de l'être dans la dernière ; et par cette raison, nous avons séparé par un trait les derniers résultats qui ont besoin d'être rectifiés.

L'avant-dernière transformée $o = y^3 - 2y^2 - y + 1$ a deux racines positives, l'une comprise entre o et 1, l'autre entre 2 et 3. Si on fait d'abord usage de la dernière, il faudra prendre 2 pour racine approchée, au lieu de 1* qui a été mis dans le tableau précédent, alors le calcul se continuera ainsi :

| | | |
|---|---|---|
| | | 5049 : 51235 |
| * $o = y^3 - 2y^2 - y + 1$ | 2 | 6296 : 63889 |
| $o = -y^3 + 3y^2 + 4y + 1$ | 4 | 17641 : 179013 |
| $o = y^3 - 20y^2 - 9y + 1$ | 20 | 76860 : 779941 |
| $o = -181 y^3 + 391 y^2 + 40 y + 1$ | 2 | 1554841 : 15777833 |
| Suivent les mêmes transformées et les mêmes quotiens que dans l'exemple I. | &c. | &c. |

Et comme on trouve ici deux nouvelles transformées dont le premier terme a pour coefficient 1, il s'ensuit que l'équation indéterminée

$$47879t^3+250158t^2u-50699tu^2+2521u^3=\pm 1$$

est susceptible de deux nouvelles solutions, savoir :

$t=17641$, $u=179013$, 2$^d$ membre $-1$
$t=76860$, $u=779941$, 2$^d$ membre $+1$.

Si ensuite on fait usage de la racine comprise entre o et 1, il faudra de plus rectifier le quotient mis devant la transformée précédente $0=y^3-4y^2+3y+1$, et on aura les résultats suivans, qui présentent le développement d'une seconde valeur de $x$ :

| | | |
|---|---|---|
| $0=y^3-4y^2+3y+1$ | 2 | 1247 : 12654<br>5049 : 51235 |
| $0=-y^3-y^2+2y+1$ | 1 | 11345 : 115124 |
| $0=y^3-3y^2-4y-1$ | 4 | 16394 : 166359 |
| $0=-y^3+20y^2+9y+1$ | 20 | 76921 : 780560 |
| $0=181y^3-391y^2-40y-1$ | 2 | 1554814 : 15777559 |
| Le reste comme ci-dessus. | 3 | &c. |
| | 1 | |
| | &c. | |

On aura donc encore trois nouvelles valeurs qui satisfont à l'équation indéterminée, savoir :

$t=11345$, $u=115124$, 2$^d$. membre $-1$
$t=16394$, $u=166359$, 2$^d$. membre $+1$
$t=76921$, $u=780560$, 2$^d$. membre $-1$.

(109) Pour éclaircir davantage cette théorie, considérons en général une équation proposée $X=0$, et supposons qu'en développant une de ses racines en fraction continue, on parvienne à une transformée quelconque $Z=0$; soit $\alpha$, $\beta$... $\mu$ &c. la série des quotiens trouvés, et $\frac{p}{q}$ la fraction convergente qui répond tant au quotient entier $\mu$ qu'au quotient-complet $z$ donné par l'équation $=0$. Voici l'opération figurée du développement :

| $X=0$ | $\alpha$ | $1:0$ |
|---|---|---|
| . | $\beta$ | $\alpha:1$ |
| . | $\gamma$ | : |
| . | $\delta$ | : |
| . | . | : |
| . | . | : |
| . | $\mu^{\circ}$ | $p^{\circ}:q^{\circ}$ |
| $Z=0$ | $\mu$ | $p:q$ |
| $Z'=0$ | $\mu'$ | $p':q'$ |
| . | . | . |
| . | . | . |
| . | . | . |

Cela posé, la transformée $Z=0$ résulte directement de la proposée, en y substituant, au lieu de $x$, la valeur $x=\frac{pz+p^{\circ}}{qz+q^{\circ}}$; réciproquement la proposée $X=0$ résulteroit d'une quelconque de ses transformées $Z=0$, en substituant dans celle-ci, au lieu de $z$, la valeur $z=\frac{q^{\circ}x-p^{\circ}}{p-qx}$. Le même rapport peut être établi entre deux transformées quelconques, pourvu que les fractions convergentes soient calculées au moyen des quotiens intermédiaires, en partant de celui qui répond à la première transformée, et qui en est une racine approchée.

Il est aisé de voir que la formule $x=\frac{pz+p^{\circ}}{qz+q^{\circ}}$ renferme implicitement toutes les racines de l'équation proposée, car on peut imaginer qu'on substitue successivement à la place de $z$ les différentes racines de l'équation $Z=0$, et il en résultera autant de différentes valeurs de $x$.

Réciproquement la valenr de $z=\frac{q^{\circ}x-p^{\circ}}{p-qx}$ renferme toutes les racines de la transformée $Z=0$. L'une de ces racines qui est positive et plus grande que l'unité, est donnée par la continuation du développement, en sorte que l'on a

$$z=\mu+\cfrac{1}{\mu'+\cfrac{1}{\mu''\ \text{\&c. à l'infini.}}}$$

Celle-ci est censée répondre à la racine $x$ qu'on a développée en fraction continue. Les autres racines de la transformée (au moins lorsque le développement est devenu régulier, et que la transformée n'a pas à-la-fois deux racines positives et plus grandes que l'unité) sont toutes négatives et plus petites que l'unité; en effet, si on désigne par $x_i$ celle des autres racines de la proposée à laquelle répond une autre racine de la transformée, désignée semblablement par $z_i$, on aura

$$z_i = \frac{q^\circ x_i - p^\circ}{p - q x_i} = -\frac{p^\circ}{p} + \frac{(pq^\circ - p^\circ q) x_i}{p(p - q x_i)}.$$

Or on a $pq^\circ - p^\circ q = \pm 1$, et comme $p$ va en augmentant, ainsi que $p - q x_i$, puisque $\frac{p}{q}$ n'est pas une fraction convergente vers $x_i$, il est clair que la valeur de $z_i$ approchera d'autant plus de $\frac{-p^\circ}{p}$ que $p$ sera grand. Ce résultat a lieu également pour toute racine de la transformée autre que $z$, d'où l'on voit que toutes ces racines tendent continuellement à être égales entr'elles, et à avoir pour valeur commune $\frac{-p^\circ}{p}$, quantité négative et plus petite que l'unité.

(110) D'un autre côté, on sait (n°. 11) que la quantité $\frac{p^\circ}{p}$ est égale à la fraction continue

$$\cfrac{1}{\mu^\circ + \cfrac{1}{\mu^{\circ\circ} + \cfrac{1}{\mu^{\circ\circ\circ} \ldots\ldots + \cfrac{1}{\alpha}}}}$$

composée des quotiens qui précèdent $\mu$ dans l'ordre rétrograde, jusqu'au premier $\alpha$ inclusivement. Donc tandis qu'une racine $z$ de la transformée $Z=0$, donne dans son développement les quotiens $\mu$, $\mu'$, $\mu''$, &c., toutes les autres racines de la même transformée donnent dans leur développement les quotiens précédens $\mu^\circ$, $\mu^{\circ\circ}$, $\mu^{\circ\circ\circ}$, &c. dans l'ordre inverse. Ces racines sont donc en effet d'autant plus près de l'égalité, qu'il y a un plus grand intervalle entre la proposée et la transformée dont il s'agit. Mais quelque approchée que

que soit cette égalité, elle ne devient jamais rigoureuse, et on peut toujours développer séparément les différentes valeurs de $z_i$ correspondantes aux valeurs analogues de $x_i$.

Car si on reforme la fraction $\frac{p'}{p}$, au moyen des quotiens qui la composent, en cette sorte

$$\mu^{\circ},\ \mu^{\circ\circ},\ \mu^{\circ\circ\circ}\ldots\ldots\ldots\ldots\ldots\ \zeta,\ \alpha$$
$$\frac{0}{1},\ \frac{1}{\mu^{\circ}}\ldots\ldots\ldots\ldots\ldots\ldots\ \frac{q^{\circ}}{q},\ \frac{p^{\circ}}{p};$$

si ensuite on met $\alpha - x_i$ à la place de $\alpha$, il est clair que la fraction continue deviendra $\frac{p^{\circ}-q^{\circ}x_i}{p-qx_i}$, et qu'ainsi on aura $-z_i = \frac{p^{\circ}-q^{\circ}x_i}{p-qx_i}$: donc la valeur exacte de $-z_i$ développée en fraction continue sera :

$$-z_i = \frac{1}{\mu^{\circ}+\frac{1}{\mu^{\circ\circ}\cdot \ddots +\frac{1}{\alpha - x_i}}}$$

Il ne s'agit plus que de substituer à la place de $x_i$ sa valeur exprimée aussi en fraction continue. Pour cela, il y a différens cas à examiner.

1°. Si $x_i$ est négatif, et que sa valeur développée commence ainsi $-x_i = \alpha_i + \frac{1}{\zeta_i + \frac{1}{\gamma_i + \&c.}}$, alors il est clair que la jonction des deux fractions continues se fera sans difficulté, et donnera

$$-z_i = \frac{1}{\mu^{\circ}+\frac{1}{\mu^{\circ\circ}+ \ddots +\frac{1}{\zeta+\frac{1}{\alpha+\alpha_i+\frac{1}{\zeta_i+\&c.}}}}}$$

2°. Si la valeur de $x_i$ est positive et moindre que $\alpha$, on fera $x_i = \alpha_i + \frac{1}{y}$, ce qui donnera $\alpha - x_i = \alpha - \alpha_i - 1 + \frac{1}{1+\frac{1}{-1+y}}$.

Dans le cas où $\alpha - \alpha_1 = 1$, il faut remonter au quotient qui précède $\alpha$, et on aura $\mathcal{C} + \frac{1}{\alpha - x_1} = \mathcal{C} + 1 + \frac{1}{-1 + y}$.

3°. Si la valeur de $x_1$ est positive et plus grande que $\alpha$, il faudra encore remonter au quotient $\mathcal{C}$, et on aura

$$\mathcal{C} + \frac{1}{\alpha - x_1} = \mathcal{C} + \frac{1}{\alpha - \alpha_1 - \frac{1}{y}}.$$

Soit d'abord $\alpha_1 = \alpha$, cette valeur se réduit à $\mathcal{C} - y$, et on se conduira à l'égard de $\mathcal{C} - y$, comme on l'a fait pour $\alpha - x$.

Soit ensuite $\alpha - \alpha_1 = -m$, on aura

$$\mathcal{C} + \frac{1}{\alpha - x_1} = \mathcal{C} - \frac{1}{m + \frac{1}{y}} = \mathcal{C} - 1 + \frac{1}{1 + \frac{1}{m - 1 + \frac{1}{y}}}.$$

De-là on voit que dans tous les cas la substitution de la valeur de $x_1$ peut se faire dans la fraction continue égale à $z_1$, sans occasionner d'autre changement que sur quelques-uns des derniers termes de la suite $\mu^{\circ}, \mu^{\circ\circ} \ldots \mathcal{C}, \alpha$, ou sur quelques-uns des premiers de la suite $\alpha_1, \mathcal{C}_1, \gamma_1$, &c. venant du développement de $x_1$. D'ailleurs la suite infinie $\alpha_1, \mathcal{C}_1, \gamma_1$, &c. (sauf peut-être quelques premiers termes) sera également comprise dans le développement de la racine $z_1$. Donc une racine quelconque de la transformée offre toujours dans son développement en fraction continue les mêmes quotiens que la racine correspondante de la proposée, sauf les premiers termes qui sont différens, tant à cause de la partie $\mu^{\circ}, \mu^{\circ\circ}$, &c. qui est propre à la transformée, qu'à cause de la jonction des deux fractions continues qui peut opérer un changement dans les premiers termes.

(111) Pour rendre ces résultats encore plus sensibles, reprenons l'exemple I, où l'équation proposée est $x^3 - x^2 - 2x + 1 = 0$, et considérons une de ses transformées, telle que

$$-197z^3 + 568z^2 + 695z + 181 = 0;$$

la racine positive et plus grande que l'unité sera donnée par les quotiens qui naissent de la continuation du développement,

et qui sont 3, 1, 6, 10, 5, 2, 2, 1, 2, 2, 1, 18, 1, 1, 3, &c.; de sorte qu'on aura pour cette première racine,

$$z = + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{10 + \cfrac{1}{5 + \text{\&c.}}}}}$$

Pour avoir les deux autres racines de la même équation, il faut, conformément à ce que nous avons dit, prendre

$$-x_{,} = \cfrac{1}{2 + \cfrac{1}{20 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 - x_{,}}}}}}$$

et substituer au lieu de $x_{,}$ successivement les deux autres racines de l'équation proposée. La racine négative étant celle dont la substitution est la plus facile, nous prendrons d'abord sa valeur développée, qui est

$$-x_{,} = 1 + \cfrac{1}{4 + \cfrac{1}{20 + \cfrac{1}{2 + \cfrac{1}{3 + \text{\&c.}}}}}$$

d'où résultera

$$-z_{,} = \cfrac{1}{2 + \cfrac{1}{20 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{20 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{6 + \text{\&c.}}}}}}}}}}}$$

Prenons ensuite la troisième racine positive

$$x_{,,} = 0 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{20 + \text{\&c.}}}}$$

si on fait pour abréger $x_{,,} = \cfrac{1}{2 + \cfrac{1}{y}}$, on aura la troisième racine de la transformée

$$-z_2=\cfrac{1}{2+\cfrac{1}{20+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1-\cfrac{1}{2+\cfrac{1}{y}}}}}}}.$$

Pour faire disparoître l'irrégularité dans cette valeur, il faut changer ainsi les derniers termes de la fraction continue :

$$\cfrac{1}{1+\cfrac{1}{1-\cfrac{1}{2+\cfrac{1}{y}}}}=\frac{y+1}{3y+2}=\cfrac{1}{2+\cfrac{y}{y+1}}=\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{y}}}.$$

Donc on aura, sans aucun terme négatif,

$$-z_2=\cfrac{1}{2+\cfrac{1}{20+\cfrac{1}{4+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{20+\cfrac{1}{2+\cfrac{1}{3+\,\&c.}}}}}}}}}$$

les quotiens suivans étant comme dans la première racine 1, 6, 10, 5, 2, 2, 1, 2, 2, 1, 18, 1, 1, 3, &c.

Au reste, si on applique cette théorie aux équations du second degré, et qu'on considère l'équation transformée qui donne la valeur du quotient-complet dans une période éloignée, on trouvera que la seconde racine de cette transformée est exprimée par les quotiens précédens pris dans l'ordre inverse; d'où il suit que la période qui a lieu dans le développement de cette seconde racine, est la même que celle de la première, mais prise dans l'ordre inverse. Résultat entièrement conforme avec ce que nous avons déjà trouvé pour les équations du second degré (§. X.).

(112) Quoiqu'on ait supposé dans ce qui précède, que les coefficiens de l'équation proposée sont des nombres entiers, cette condition n'est pas cependant absolument nécessaire, et on peut, au besoin, convertir en fraction continue la racine de toute équation proposée, soit algébrique, soit même transcendante. Pour cela, il faut chercher, par une méthode quelconque, la valeur approchée

de la racine dont il s'agit, puis convertir cette valeur en fraction continue, en ayant soin d'arrêter le développement et le calcul des fractions convergentes au point où l'on présume que l'exactitude doit cesser. Si la fraction $\frac{p}{q}$ à laquelle on s'arrête, est une fraction convergente, il faut se rappeler que la différence de cette fraction avec $x$ doit être moindre que $\frac{1}{q^2}$; et ainsi le degré d'approximation de la valeur de $x$ étant supposé connu, on connoîtra la limite de $q$. Au reste, une approximation ultérieure serviroit à redresser l'erreur, s'il y en avoit.

Supposons donc qu'en vertu de la première approximation, on a trouvé les quotiens et les fractions convergentes vers $x$ comme il suit :

Quotiens......... $\alpha$, $\beta$, $\gamma$ ....... $\mu^\circ$

Fract. converg..... $\frac{1}{0}$, $\frac{\alpha}{1}$, $\frac{\alpha\beta+1}{\beta}$..... $\frac{p^\circ}{q^\circ}$, $\frac{p}{q}$.

Pour continuer le développement, on prendra l'équation proposée $F(x)=0$, et on substituera dans le premier membre, au lieu de $x$, la valeur $\frac{p}{q}+\omega$. On suppose que $\omega$ est une correction assez petite pour qu'on puisse négliger les puissances de $\omega$ supérieures à la première, et alors en faisant $\frac{dF}{dx}=F'$, le résultat de la substitution sera $F:\left(\frac{p}{q}\right)+\omega F':\left(\frac{p}{q}\right)=0$, d'où l'on tire

$$\omega=-\frac{F:\left(\frac{p}{q}\right)}{F':\left(\frac{p}{q}\right)}$$

Soit maintenant $z$ le quotient-complet qui répond à $\frac{p}{q}$, on aura $x=\frac{pz+p^\circ}{qz+q^\circ}=\frac{p}{q}+\omega$, ce qui donnera, en substituant la valeur de $\omega$,

$$z=-\frac{q^\circ}{q}+(pq^\circ-p^\circ q)\cdot\frac{F'\left(\frac{p}{q}\right)}{q\;F\left(\frac{p}{q}\right)}$$

Si l'équation est algébrique, et qu'on ait

$$F:(x) = ax^n + bx^{n-1} + cx^{n-2} + \ldots\ldots\ldots\ldots + k$$

$$F':(x) = nax^{n-1} + (n-1)bx^{n-2} + (n-2)cx^{n-3} + \&c.$$

il en résultera

$$z = -\frac{q^\circ}{q} + \frac{pq^\circ - p^\circ q}{q} \cdot \frac{nap^{n-1} + (n-1)bp^{n-2}q + (n-2)cp^{n-3}q^2 + \&c.}{ap^n + bp^{n-1}q + cp^{n-2}q^2 + \ldots\ldots + kq^n}$$

ce qui revient à la formule du n°. 100.

En général, il est à remarquer que la valeur de $z$ donnera par son développement divers quotiens $\mu$, $\mu'$, $\mu''$, &c. qui feront suite avec les quotiens déjà trouvés, et permettront de continuer le calcul des fractions convergentes jusqu'à ce que l'erreur de la première approximation soit réduite à son quarré. Et s'il arrivoit que la valeur de $z$ ne fût pas positive et plus grande que l'unité, ce seroit une preuve qu'un ou plusieurs des quotiens précédens $\mu^\circ$, $\mu^{\circ\circ}$, &c. sont fautifs, et doivent être corrigés au moyen de la valeur de $z$. Alors on réduiroit en une seule fraction $\mu^\circ + \frac{1}{z}$, et si la somme étoit positive et plus grande que l'unité, il n'y auroit que le dernier quotient $\mu^\circ$ à changer. Dans le cas contraire, il faudroit substituer la valeur de $z$ dans $\mu^{\circ\circ} + \cfrac{1}{\mu^\circ + \cfrac{1}{z}}$, ou même dans $\mu^{\circ\circ\circ} + \cfrac{1}{\mu^{\circ\circ} + \cfrac{1}{\mu^\circ + \cfrac{1}{z}}}$ et ainsi en rétrogradant, jusqu'à ce qu'on parvînt à un résultat positif et plus grand que l'unité. Cette valeur étant développée en fraction continue, donneroit à-la-fois les quotiens qu'on doit substituer aux quotiens défectueux et quelques-uns de ceux qui les suivent, selon le degré de la première approximation.

Il est clair que par des opérations semblables, réitérées autant qu'il est nécessaire, on peut parvenir à développer en fraction continue, et jusqu'à un nombre de quotiens quelconque, toute racine d'une équation proposée, de quelque nature qu'elle soit.

(113) Quant à la méthode pour obtenir la première approximation, on peut proposer comme l'une des plus simples et des plus convenables pour cet objet, la méthode de Daniel Bernoulli, fondée sur la théorie des suites récurrentes, et dont Euler a donné

une exposition détaillée dans son *Introd. in Analys. Cap. XVII.* Cependant comme cette méthode est sujette à quelques difficultés dans les applications, il ne sera pas inutile de la présenter ici avec une modification qui peut faire disparoître une grande partie de ces difficultés.

Soit $x^m + ax^{m-1} + bx^{m-2} + cx^{m-3} + \&c. = 0$, une équation proposée dont les racines sont $\alpha$, $\beta$, $\gamma$, $\delta$, &c; si on prend pour $z$ une variable quelconque, on aura l'équation identique

$$1 + az + bz^2 + cz^3 + \&c. = (1-\alpha z)(1-\beta z)(1-\gamma z)\ \&c.;$$

d'où résulte, par la différentiation, cette autre équation pareillement identique:

$$\frac{-a-2bz-3cz^2-\&c.}{1+az+bz^2+cz^3+\&c.} = \frac{\alpha}{1-\alpha z} + \frac{\beta}{1-\beta z} + \frac{\gamma}{1-\gamma z} + \frac{\delta}{1-\delta z} + \&c.$$

Soit $A + Bz + Cz^2 + Dz^3 \ldots + Mz^{n-1} + Nz^n + \&c.$ la série qui vient du développement du premier membre, on aura, d'après la loi connue des suites récurrentes:

$$A = -a$$
$$B = -aA - 2b$$
$$C = -aB - bA - 3c$$
$$D = -aC - bB - cA - 4d$$
$$E = -aD - bC - cB - dA - 5e$$
&c.

Il faut par conséquent que la suite ainsi trouvée $A + Bz + Cz^2 + \&c.$ soit identique avec celle qui résulte du second membre $\frac{\alpha}{1-\alpha z} + \frac{\beta}{1-\beta z} + \&c.$ Or on a $\frac{\alpha}{1-\alpha z} = \alpha + \alpha^2 z + \alpha^3 z^2 + \&c.$, et les autres fractions partielles donnent des résultats semblables; donc en réunissant tous ces résultats on aura

$$A = \alpha + \beta + \gamma + \delta + \varepsilon + \&c.$$
$$B = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 + \varepsilon^2 + \&c.$$
$$C = \alpha^3 + \beta^3 + \gamma^3 + \delta^3 + \varepsilon^3 + \&c.$$

.
.
.

et en général $N = \alpha^n + \beta^n + \gamma^n + \delta^n + \varepsilon^n + \&c.$

Ces formules sont les mêmes dont on se sert pour trouver la somme des puissances de même nom des racines d'une équation donnée; mais il est évident qu'elles sont applicables aussi à la résolution approchée des équations; car si $\alpha$ est la plus grande des racines, et que l'exposant $n$ soit suffisamment grand, on aura à fort peu-près $N=\alpha^n$ : on auroit, par la même raison, $M=\alpha^{n-1}$, donc la racine cherchée $\alpha=\frac{N}{M}$.

Donc pour avoir par approximation la plus grande racine de l'équation proposée, il faut calculer les coefficiens successifs $A, B, C, D \ldots M, N \ldots$ par la loi générale des suites récurrentes; puis on divisera le dernier coefficient trouvé par l'avant-dernier, et le résultat sera la valeur de la racine demandée : valeur d'autant plus approchée, que l'opération aura été poussée plus loin, et qu'il y aura plus d'inégalité entre les racines.

Il est aisé, par une transformation, de faire en sorte qu'une racine quelconque devienne la plus grande des racines, ainsi cette méthode peut servir à trouver indistinctement toutes les racines. Dans un grand nombre de cas l'approximation sera plus rapide par cette voie que par aucune autre connue; quelquefois elle sera lente, quelquefois aussi les résultats seront absolument fautifs; mais il est facile de prévoir et d'éviter ces inconvéniens, si l'on a une première notion de la grandeur relative et de la nature des racines.

(114) Appliquons ces méthodes à l'équation $x^3-3x^2+1=0$; pour avoir la valeur approchée de la plus grande racine, il faudra développer en série la fraction $\frac{3-3z^2}{1-3z+z^3}$, ce qui donnera $3+9z+24z^2+69z^3+198z^4+570z^5+1641z^6+4725z^7+13605z^8+39174z^9+$ &c. En s'arrêtant ainsi au dixième terme, on aura la racine cherchée $x=\frac{39174}{13605}$.

Maintenant si on développe cette valeur en fraction continue, on aura les quotiens 2, 1, 7, 3, 2, 3, 1, 2, 6; et pour juger jusqu'à quel point ils peuvent être exacts, on développera semblablement la fraction $\frac{13605}{4725}$ qu'on auroit eue en s'arrêtant au neuvième

vième terme ; il résulte de celle-ci les quotiens 2, 1, 7, 3, 2, 5 ; d'où il paroît qu'on peut regarder comme exacts les quotiens 2, 1, 7, 3, 2, 3. Au moyen de ceux-ci on calculera les fractions convergentes vers $x$ comme il suit :

Quotiens.......... 2, 1, 7, 3, 2, 3

Fract. converg..... $\frac{1}{0}, \frac{2}{1}, \frac{3}{1}, \frac{23}{8}, \frac{72}{25}, \frac{167}{58}, \frac{573}{199}$.

Pour continuer le calcul de ces fractions d'après la méthode du n°. 112, faisons $\frac{p^\circ}{q^\circ}=\frac{167}{58}$, $\frac{p}{q}=\frac{573}{199}$, et soit toujours $z$ le quotient-complet qui répond à cette dernière fraction, nous aurons (en observant que $pq^\circ-p^\circ q=+1$)

$$z=-\frac{q^\circ}{q}+\frac{1}{q}\cdot\frac{3p^\circ-6pq}{p^3-3p^\circ q+q^3}=\frac{260051}{139897}.$$

Cette valeur étant positive et plus grande que l'unité, il s'ensuit que tous les quotiens déjà trouvés sont exacts ; et pour avoir ceux qui viennent à la suite, il faut développer la valeur de $z$ en fraction continue, ce qui donnera les nouveaux quotiens 1, 1, 6, 11, 1, 1, 1, 3, &c.; de sorte que l'opération du développement de $x$ se continuera ainsi :

Quot. .. 1, 1, 6, 11, 1,

Fr. conv. $\frac{167}{58}, \frac{573}{199}, \frac{740}{257}, \frac{1313}{456}, \frac{8618}{2993}, \frac{96111}{33379}, \frac{104729}{36372}$, &c.

On s'arrête à cette dernière, parce que 104729 approche déjà du quarré de 573, et que la fraction suivante pourroit bien n'être plus du nombre des fractions convergentes. On continuera ensuite l'approximation plus loin, si on le juge à propos, en réitérant de semblables calculs.

(115) Les méthodes qu'on vient d'exposer ne laissent rien à desirer pour ce qui regarde les racines réelles des équations. Quant aux racines imaginaires, il peut être utile aussi d'en avoir une expression approchée indéfiniment, et l'analyse indéterminée offre des cas où l'on a besoin de convertir en fraction continue la partie réelle de ces racines. Nous saisirons cette occasion de présenter

quelques vues nouvelles sur l'approximation des racines imaginaires, objet jusqu'à présent assez négligé des Analystes.

On sait que toute racine imaginaire d'une équation peut être représentée par $\alpha+\mathcal{C}\sqrt{-1}$, $\alpha$ et $\mathcal{C}$ étant des quantités réelles; on sait aussi que la quantité $\alpha$ peut être déterminée directement par une équation du degré $\frac{n.n-1}{2}$, $n$ étant le degré de l'équation proposée. Ayant trouvé $\alpha$, il n'est pas difficile d'avoir $\mathcal{C}$, car comme l'équation proposée doit être divisible par $x^2-2\alpha x+\alpha^2+\mathcal{C}^2$, si on exécute la division par ce polynome, et que le reste soit $Ax+B$, il faudra qu'on ait $A=0$ et $B=0$, équations entre $\alpha$ et $\mathcal{C}$, au moyen desquelles il est facile d'avoir une valeur rationnelle de $\mathcal{C}^2$. Tout se réduit donc à trouver la valeur de $\alpha$ par l'équation dont elle dépend; mais dès que $n$ surpasse 3 ou 4, le degré de cette équation devient trop élevé, pour qu'elle soit de quelqu'utilité dans la pratique, et il faut absolument recourir à d'autres moyens pour avoir les valeurs approchées de $\alpha$ et $\mathcal{C}$. Or quels que soient $\alpha$ et $\mathcal{C}$, on peut toujours supposer $\alpha=\theta\cos\varphi$, $\mathcal{C}=\theta\sin\varphi$, ce qui donnera $x=\theta(\cos\varphi+\sqrt{-1}\sin\varphi)$, et en général $x^m=\theta^m(\cos m\varphi+\sqrt{-1}\sin m\varphi)$. C'est par ces formules, dont l'emploi a été indiqué par Euler, qu'on pourra parvenir à simplifier beaucoup la recherche des racines imaginaires.

Considérons d'abord l'équation $ax^m+bx+c=0$ à laquelle peut se réduire toute équation à trois termes; (car la solution que nous allons donner ne suppose pas que $m$ soit un nombre entier). Si on met au lieu de $x$ sa valeur $\theta(\cos\varphi+\sqrt{-1}\sin\varphi)$, l'équation proposée se décomposera en ces deux autres :

$$a\theta^m\cos m\varphi+b\theta\cos\varphi+c=0$$
$$a\theta^m\sin m\varphi+b\theta\sin\varphi=0.$$

Multipliant la première par $\sin m\varphi$, la seconde par $-\cos m\varphi$, et ajoutant les produits, on aura

$$c\sin m\varphi+b\theta(\sin m\varphi\cos\varphi-\sin\varphi\cos m\varphi)=0,$$

ou $c\sin m\varphi+b\theta\sin(m-1)\varphi=0$; d'où l'on tire

$$\theta=\left(-\frac{c}{b}\right)\cdot\frac{\sin m\varphi}{\sin(m-1)\varphi}.$$

Cette valeur étant substituée dans la seconde des équations en $\varphi$ et $\theta$, on aura pour déterminer $\varphi$ l'équation,

$$\frac{\sin^m m\varphi}{\sin\varphi \sin^{m-1}(m-1)\varphi} = \frac{c}{a}\left(-\frac{b}{c}\right)^m.$$

Or après quelques essais, on reconnoîtra bientôt entre quels degrés voisins tombe l'angle $\varphi$ ; ensuite par les fausses positions il ne faudra que très-peu de calcul pour déterminer $\varphi$ avec toute l'exactitude que les tables comportent, c'est-à-dire, ordinairement avec six ou sept chiffres : $\varphi$ étant connu, $\theta$ le sera, et ainsi on connoîtra la racine imaginaire $\theta(\cos\varphi + \sqrt{-1}\sin\varphi)$ assez exactement pour la plupart des applications.

(116) Prenons pour exemple l'équation $x^4 - x + 1 = 0$; en faisant $x = \theta(\cos\varphi + \sqrt{-1}\sin\varphi)$, on aura $\theta = \frac{\sin 4\varphi}{\sin 3\varphi}$, et l'équation pour déterminer $\varphi$ sera

$$\frac{\sin^4 . 4\varphi}{\sin\varphi . \sin^3 . 3\varphi} = 1.$$

Si l'on fait $\varphi = 30°$, le premier membre se réduira à $\frac{9}{8}$, et ainsi l'erreur sera $+\frac{1}{8}$; si l'on fait $\varphi = 31°$, le premier membre deviendra 0,921, ce qui donne l'erreur $-0,079$. De-là on trouve $\varphi = 30° 36'$ et une fraction.

Soit donc $\varphi = 30° 36'$, le premier membre aura pour logarithme 9,999933, et l'erreur sera par conséquent de $-67$ unités décimales du sixième ordre, d'où l'on voit qu'il faut diminuer légèrement la valeur de $\varphi$ au lieu de l'augmenter. Je fais $\varphi = 30° 35'$, et j'ai le logarithme du premier membre 0,001394; ce qui donne l'erreur $+1394$; de-là on tire la vraie valeur de $\varphi$ approchée autant que le permettent des tables à six décimales :

$$\varphi = 30° 35', 954 ;$$

ensuite on aura $L.\theta = 9,926739$, $L.\alpha = 9,861615$, $L.c = 9,633482$. Donc enfin la racine cherchée

$$x = 0,727136 + 0,430014\sqrt{-1}.$$

La partie réelle étant réduite en fraction continue donne les quotiens et les fractions convergentes comme il suit :

X 2

Quotiens..... 0, 1, 2, 1, 1, 1, 59, 1, &c.

Fract. converg. $\frac{1}{0}$, $\frac{0}{1}$, $\frac{1}{1}$, $\frac{2}{3}$, $\frac{3}{4}$, $\frac{5}{7}$, $\frac{8}{11}$, $\frac{477}{656}$, $\frac{485}{667}$, &c.

(117) Considérons maintenant l'équation générale

$$ax^n+bx^{n-1}+cx^{n-2}+\ldots\ldots+hx+k=0;$$

si on y substitue au lieu de $x$ la valeur $\theta(\cos\varphi+\sqrt{-1}\sin\varphi)$, et qu'on fasse, pour abréger,

$$P=a\theta^n\cos n\varphi+b\theta^{n-1}\cos(n-1)\varphi+c\theta^{n-2}\cos(n-2)\varphi\ldots+h\theta\cos\varphi+k$$
$$Q=a\theta^n\sin n\varphi+b\theta^{n-1}\sin(n-1)\varphi+c\theta^{n-2}\sin(n-2)\varphi\ldots+h\theta\sin\varphi,$$

le résultat de la substitution sera $P+Q\sqrt{-1}=0$, de sorte qu'on aura, pour déterminer $\theta$ et $\varphi$, les deux équations $P=0$, $Q=0$. Mais comme la résolution effective de ces équations n'est possible que dans un petit nombre de cas particuliers, qui ne s'étendent guères au-delà du théorême de Côtes, il faut se borner à les résoudre par approximation.

Supposons donc qu'après quelques tentatives on a trouvé des valeurs de $\varphi$ et de $\theta$ qui rendent $P$ et $Q$ presque nulles; pour avoir des valeurs plus approchées, on désignera celles-ci par $\varphi+d\varphi$ et $\theta+d\theta$; il faudra donc que la substitution de $\varphi+d\varphi$ et $\theta+d\theta$ à la place de $\varphi$ et $\theta$ dans les fonctions $P$ et $Q$, rende ces fonctions égales à zéro. Or, en négligeant les puissances de $d\theta$ et $d\varphi$ supérieures à la première, la quantité $P$ devient en général, par la substitution dont il s'agit, $P+\frac{dP}{d\theta}d\theta+\frac{dP}{d\varphi}d\varphi$, et les valeurs des coefficiens sont :

$$\theta\frac{dP}{d\theta}=na\theta^n\cos n\varphi+(n-1)b\theta^{n-1}\cos(n-1)\varphi\ldots\ldots\ldots+h\theta\cos\varphi$$
$$\frac{dP}{d\varphi}=-na\theta^n\sin n\varphi-(n-1)b\theta^{n-1}\sin(n-1)\varphi\ldots\ldots\ldots-h\theta\sin\varphi.$$

De même la quantité $Q$ devenant $Q+\theta\frac{dQ}{d\theta}.\frac{d\theta}{\theta}+\frac{dQ}{d\varphi}d\varphi$, on a

$$\theta\frac{dQ}{d\theta}=na\theta^n\sin n\varphi+(n-1)b\theta^{n-1}\sin(n-1)\varphi\ldots\ldots\ldots+h\theta\sin\varphi$$
$$\frac{dQ}{d\varphi}=na\theta^n\cos n\varphi+(n-1)b\theta^{n-1}\cos(n-1)\varphi\ldots\ldots+h\theta\cos\varphi.$$

Donc il suffit de prendre deux auxiliaires $M$ et $N$ d'après les formules

$$M = na\theta^n \cos n\varphi + (n-1)b\theta^{n-1}\cos(n-1)\varphi \ldots\ldots + h\theta\cos\varphi$$
$$N = na\theta^n \sin n\varphi + (n-1)b\theta^{n-1}\sin(n-1)\varphi \ldots\ldots + h\theta\sin\varphi;$$

et on aura, pour déterminer $\frac{d\theta}{\theta}$ et $d\varphi$, les deux équations

$$P + M\frac{d\theta}{\theta} - N d\varphi = 0$$

$$Q + N\frac{d\theta}{\theta} + M d\varphi = 0,$$

d'où l'on tire

$$-\frac{d\theta}{\theta} = \frac{PM + QN}{MM + NN}\ , \quad d\varphi = \frac{PN - QM}{MM + NN}.$$

On connoîtra ainsi les valeurs corrigées de $\theta$ et $\varphi$ qui sont $\theta\left(1 + \frac{d\theta}{\theta}\right)$, et $\varphi + d\varphi$, où l'on doit observer que la valeur de $d\varphi$ donnée par la formule, est exprimée en parties du rayon, et que pour la réduire en minutes ou en secondes, il faut la multiplier par le nombre de minutes ou de secondes contenues dans le rayon. Enfin on peut rendre ces formules encore plus commodes pour le calcul trigonométrique, en prenant des angles $\varpi$, $\lambda$ et des nombres $\Pi$, $\Lambda$, tels qu'on ait :

$$\text{Tang}\,\varpi = \frac{P}{Q}\ , \quad \Pi = \frac{P}{\sin\varpi} = \frac{Q}{\cos\varpi}$$
$$\text{Tang}\,\lambda = \frac{M}{N}\ , \quad \Lambda = \frac{M}{\sin\lambda} = \frac{N}{\cos\lambda};$$

d'où résultera

$$\frac{d\theta}{\theta} = -\frac{\Pi}{\Lambda}\cos(\varpi - \lambda)\ , \quad d\varphi = \frac{\Pi}{\Lambda}\sin(\varpi - \lambda).$$

Il faut bien remarquer que les quantités $M$ et $N$ sont très-faciles à former par le moyen des mêmes termes qui servent à composer les valeurs de $P$ et $Q$ ; car tandis que $P$, par exemple, est exprimé par la suite des termes

$$A + B + C + D + \&c.,$$

où l'on a $\mathcal{A} = a\theta^n \cos n\varphi$, $B = b\,\theta^{n-1}\cos(n-1)\varphi$, &c. la valeur de $M$ l'est par la suite

$$n\mathcal{A} + (n-1)B + (n-2)C + (n-3)D + \&c.$$

La valeur de $N$ se conclut de même de celle de $Q$.

Ayant trouvé des valeurs plus approchées de $\theta$ et $\varphi$, on peut se servir de celles-ci pour en trouver de nouvelles qui soient encore plus approchées, et ainsi de suite, jusqu'à ce qu'on obtienne le degré d'exactitude dont les tables sont susceptibles.

(118) Appliquons cette méthode à l'équation $x^4 - x + 1 = 0$ dont nous nous sommes déjà occupés. En faisant toujours $x = \theta(\cos\varphi + \sqrt{-1}\sin\varphi)$, on peut prendre pour premières valeurs approchées $\varphi = 30°$, $\theta = \sin 60° = \frac{1}{2}\sqrt{3}$, il en résulte

$$P = \theta^4\cos 4\varphi - \theta\cos\varphi + 1 = -\frac{9}{32} - \frac{3}{4} + 1 = -\frac{1}{32}$$

$$M = 4\theta^4\cos 4\varphi - \theta\cos\varphi \quad = -\frac{9}{8} - \frac{3}{4} \quad = -\frac{15}{8}$$

$$Q = \theta^4\sin 4\varphi - \theta\sin\varphi \quad = \frac{9}{32}\sqrt{3} - \frac{1}{4}\sqrt{3} = \frac{\sqrt{3}}{32}$$

$$N = 4\theta^4\sin 4\varphi - \theta\sin\varphi = \frac{9}{8}\sqrt{3} - \frac{1}{4}\sqrt{3} = \frac{7}{8}\sqrt{3}.$$

Donc $\dfrac{d\theta}{\theta} = -\left(\dfrac{PM+QN}{MM+NN}\right) = -\dfrac{36}{8.186} = -\dfrac{3}{124}$,

et $d\varphi = \dfrac{PN-QM}{MM+NN} = \dfrac{\sqrt{3}}{186} = 0°\ 32'$.

Les valeurs corrigées de $\theta$ et $\varphi$ seront par conséquent

$$\theta = \tfrac{1}{2}\sqrt{3}\left(1 - \frac{3}{124}\right) = 0{,}845 \text{ et } \varphi = 30°\ 32'.$$

Avec ces valeurs corrigées, on calculera de nouvelles valeurs de $P$, $M$, $Q$, $N$, lesquelles seront :

$$P = -0{,}271176 - 0{,}727827 + 1 = 0{,}000997$$
$$M = -1{,}084704 - 0{,}727827 \quad = -1{,}8125$$
$$Q = \quad 0{,}431733 - 0{,}429294 \quad = 0{,}002439$$
$$N = \quad 1{,}726932 - 0{,}429294 \quad = 1{,}2976;$$

d'où l'on tire

$$d\theta = -0{,}000231 \qquad d\varphi = \ldots\ 3',953$$
$$\theta = 0{,}845 \qquad \varphi = 30°\,32'$$
$$\theta \text{ corrigé } = 0{,}844769 \qquad \varphi \text{ corrigé} = 30°\,35',953.$$

Résultat conforme à celui que nous avons déjà trouvé n°. 116.

(119) Cette méthode ne peut donner qu'un degré d'exactitude borné, et avec les tables les plus étendues, on ne trouvera que les dix premiers chiffres des nombres $\varphi$ et $\theta$, ou des quantités $\alpha$ et $\beta$ qui en dépendent. Si on a besoin d'une plus grande approximation, il faudra cesser de se servir des sinus, et rétablir la racine cherchée sous la forme $x = \alpha + \beta\sqrt{-1}$. Nous supposerons donc qu'on connoît déjà, par le procédé qui vient d'être expliqué, ou par tout autre moyen, des valeurs déjà fort approchées de $\alpha$ et $\beta$, et il s'agit d'en chercher de nouvelles, qui soient beaucoup plus approchées.

Si on fait en général $(\alpha+\beta\sqrt{-1})^n = F_n + G_n\sqrt{-1}$, ou si on représente par $F_n$ et $G_n$ les quantités réelles développées

$$F_n = \alpha^n - \frac{n.n-1}{1.2}\alpha^{n-2}\beta^2 + \frac{n.n-1.n-2.n-3}{1.2.3.4}\alpha^{n-4}\beta^4 - \&c.$$

$$G_n = n\alpha^{n-1}\beta - \frac{n.n-1.n-2}{1.2.3}\alpha^{n-3}\beta^3 + \&c.$$

la quantité $F_n$ sera ce qui a été représenté ci-dessus par $\theta^n \cos n\varphi$, et $G_n$ sera pareillement $\theta^n \sin n\varphi$, car on a aussi $\alpha+\beta\sqrt{-1} = \theta(\cos\varphi + \sqrt{-1}\sin\varphi)$, $(\alpha+\beta\sqrt{-1})^n = \theta^n(\cos n\varphi + \sqrt{-1}\sin n\varphi)$. Donc on pourra faire comme ci-dessus (n°. 117)

$$P = aF_n + bF_{n-1} + cF_{n-2} \ldots\ldots\ldots\ldots + hF_1 + k$$
$$= naF_n + (n-1)bF_{n-1} + (n-2)cF_{n-2} + \ldots\ldots + hF_1$$

$$Q = aG_n + bG_{n-1} + cG_{n-2} + \ldots\ldots\ldots\ldots + hG_1$$
$$N = naG_n + (n-1)bG_{n-1} + (n-2)cG_{n-2} + \ldots\ldots + hG_1,$$

et de-là on déduira également

$$-\frac{d\theta}{\theta} = \frac{PM+QN}{MM+NN}, \quad d\varphi = \frac{PN-QM}{MM+NN}.$$

Or on a $\alpha = \theta \cos \varphi$, et $\zeta = \theta \sin \varphi$; donc

$$d\alpha = \alpha \frac{d\theta}{\theta} - \zeta d\varphi, \text{ et } d\zeta = \zeta \frac{d\theta}{\theta} + \alpha d\varphi,$$

et ainsi en substituant les valeurs de $\frac{d\theta}{\theta}$ et $d\varphi$, on aura directement :

$$d\alpha = -\alpha . \left(\frac{PM+QN}{MM+NN}\right) - \zeta . \left(\frac{PN-QM}{MM+NN}\right)$$

$$d\zeta = -\zeta \left(\frac{PM+QN}{MM+NN}\right) + \alpha . \left(\frac{PN-QM}{MM+NN}\right).$$

Ces formules sont aussi simples qu'on peut le desirer ; car si on a les valeurs approchées de $\alpha$ et $\zeta$, et qu'on veuille les vérifier par la substitution, il faut calculer tous les termes des quantités $P$ et $Q$, afin de voir si leur somme se réduit à zéro ; or les termes calculés de $P$ et $Q$ font connoître ceux de $M$ et $N$, au moyen d'une simple multiplication par l'indice de chaque terme ; il ne faut donc presqu'aucun calcul pour obtenir les valeurs de $M$ et $N$, dont dépendent les corrections $d\alpha$ et $d\zeta$. Nous observerons cependant qu'on doit calculer les valeurs de $P$ et $Q$ avec deux fois plus de chiffres lorsqu'on veut continuer l'approximation, que lorsqu'on veut simplement vérifier la racine trouvée $\alpha + \zeta\sqrt{-1}$ ; mais quant aux valeurs de $M$ et $N$, il suffit de les calculer avec autant de chiffres qu'il y en a d'exacts dans $\alpha$ et $\zeta$. Ces préceptes, ou des préceptes semblables, sont communs à toutes les méthodes d'approximation.

§. XV.

## §. XV. *Résolution en nombres entiers de l'équation indéterminée* $Ly^n + My^{n-1}z + Ny^{n-2}z^2 \ldots + Vz^n = \pm H$.

(120) Nous supposerons que cette équation a été préparée de la manière indiquée n°. 67, et qu'en conséquence on peut considérer $y$ et $z$ comme premiers entr'eux, ainsi que $z$ et $H$. Cela posé, on pourra faire semblablement $y = \theta z + Hu$, $\theta$ étant un nombre compris entre $-\frac{1}{2}H$ et $+\frac{1}{2}H$; substituant cette valeur dans l'équation proposée, et divisant tout par $H$, on aura

$$\begin{aligned} \pm 1 = & \left(\frac{L\theta^n + M\theta^{n-1} + N\theta^{n-2} \ldots + V}{H}\right) z^n \\ & + (nL\theta^{n-1} + (n-1)M\theta^{n-2} + \&c.) z^{n-1} u \\ & + \left(\frac{n.n-1}{2} L\theta^{n-2} + \frac{n-1.n-2}{2} M\theta^{n-3} + \&c.\right) H z^{n-2} u^2 \\ & + \&c. \end{aligned}$$

Mais $z$ et $H$ étant premiers entr'eux, cette équation ne peut subsister, à moins que $\frac{L\theta^n + M\theta^{n-1} + N\theta^{n-2} \ldots + V}{H}$ ne soit un nombre entier; c'est la condition qui sert à déterminer $\theta$. On essaiera donc successivement pour $\theta$ tous les nombres entiers compris depuis $-\frac{1}{2}H$ jusqu'à $+\frac{1}{2}H$, et s'il n'en est aucun qui rende $L\theta^n + M\theta^{n-1} + N\theta^{n-2} +$ &c. divisible par $H$, on en conclura avec certitude que l'équation proposée n'est pas résoluble en nombres entiers; mais si on trouve un ou plusieurs nombres qui satisfont à cette condition, on aura à résoudre ultérieurement, pour chaque valeur de $\theta$, la transformée en $z$ et $u$, qui sera de la forme

$$az^n + bz^{n-1}u + cz^{n-2}u^2 + \ldots + ku^n = \pm 1;$$

et il est évident que chaque solution de celle-ci en nombres entiers en donnera une de la proposée.

Tout se réduit par conséquent à résoudre une équation de même forme que l'équation proposée, mais dans laquelle le second membre $= \pm 1$.

On doit supposer que le premier membre de l'équation proposée (avant même d'y appliquer aucune réduction) n'est divisible par aucun facteur rationnel; car s'il pouvoit se partager en deux facteurs de cette sorte, l'un du degré $m$, l'autre du degré $n-m$, l'équation proposée se décomposeroit en deux autres de la forme

$$L'y^m + M'y^{m-1}z + N'y^{m-2}z^2 + \&c. = \pi$$
$$L''y^{n-m} + M''y^{n-m-1}z + N''y^{n-m-2}z^2 + \&c. = \frac{H}{\pi},$$

$\pi$ étant un diviseur de $H$, de sorte qu'alors le problême deviendroit entièrement déterminé.

Il s'ensuit évidemment de cette supposition, que le premier membre $az^n + bz^{n-1}u + cz^{n-2}u^2 + \&c.$ de la transformée, n'est point non plus décomposable en facteurs rationnels. Donc il n'y aura aucnnes valeurs de $u$ et $z$ en nombres entiers qui pourront rendre ce premier membre égal à zéro; et ainsi la valeur $\pm 1$ est absolument la plns petite de toutes celles qu'il peut recevoir en substituant pour $y$ et $z$ des nombres entiers quelconques positifs ou négatifs.

(121) Cela posé, nous allons chercher en général quelles doivent être les valeurs de $t$ et $u$ pour que la fonction homogène

$$at^n + bt^{n-1}u + ct^{n-2}u^2 \ldots\ldots + ku^n$$

soit la plus petite possible. Ponr cela, imaginons qu'en résolvant l'équation déterminée

$$0 = ax^n + bx^{n-1} + cx^{n-2} \ldots\ldots + k$$

on trouve les facteurs simples réels $x-\alpha$, $x-\alpha'$, $x-\alpha''$, &c. et les facteurs doubles imaginaires $(x-6)^2+\gamma^2$, $(x-6')^2+\gamma'^2$, &c.; alors la fonction proposée $at^n + bt^{n-1}u + ct^{n-2}u^2 + \&c.$ que je désigne par $F(t, u)$, sera égale au produit

$$a(t-\alpha u)(t-\alpha' u)(t-\alpha'' u)\ldots\left(\overline{t-6u}^2+\gamma^2u^2\right)\left(\overline{t-6'u}^2+\gamma'^2u^2\right)\&c.$$

Supposons que les valeurs de $t$ et $u$ qui répondent au *minimum* de cette fonction soient $t=p$, $u=q$, en sorte que ce *minimum* soit

$$F(p, q) = a(p-\alpha q)(p-\alpha' q)\ldots\left(\overline{p-6q}^2+\gamma^2q^2\right)\&c.$$

Il faudra donc qu'en prenant pour $t$ et $u$ des valeurs en nombres entiers différentes de $p$ et $q$ (au moins jusqu'à une certaine limite), on ait $F(p, q) < F(t, u)$. C'est ce qui ne pourroit avoir lieu, si

chaque facteur de $F(t,u)$ étoit égal ou plus petit que le facteur correspondant de $F(p,q)$. Donc il y aura au moins un facteur de $F(t,u)$ qui sera plus grand que le facteur correspondant de $F(p,q)$. Ce facteur sera, ou l'un des facteurs simples réels, on l'un des facteurs doubles imaginaires.

1°. Soit $t-\alpha u$ le facteur simple plns grand que son correspondant $p-\alpha q$; comme les nombres $t$ et $u$ ont été pris à volonté, et qn'on pent supposer par conséqnent que $\frac{t}{u}$ diffère très-peu de $\frac{p}{q}$, il en résulte que $\frac{p}{q}$ doit être une fraction très-approchée de $\alpha$, et on peut même conjecturer de-là que $\frac{p}{q}$ doit être l'une des fractions convergentes vers la racine $\alpha$. En effet, si $\frac{p^{\circ}}{q^{\circ}}, \frac{p}{q}, \frac{p'}{q'}$ sont troisfractions consécutives convergentes vers $\alpha$, il a été démontré n°. 8, que quels qne soient les nombres $t$ et $u$, pourvn seulement que $u$ soit moindre que $q'$, la quantité $t-\alpha u$ sera tonjours plus grande que $p-\alpha q$, ce qui satisferoit à la condition observée.

2°. Soit $(t-\zeta u)^2+\gamma^2 u^2$ le factenr double imaginaire plus grand que son correspondant $(p-\zeta q)^2+\gamma^2 q^2$; nous supposerons qu'on a pris $u<q$, alors il faudra à plus forte raison que $t-\zeta u$ soit plus grand que $p-\zeta q$. Or c'est ce qui aura lieu, si $\frac{p}{q}$ est l'une des fractions convergentes vers la quantité $\zeta$, partie réelle de la racine imaginaire $\zeta\pm\gamma\sqrt{-1}$.

(122) Revenons à la considération du premier cas, et supposons qu'on ait pris $t=p^{\circ}, u=q^{\circ}$, $\frac{p^{\circ}}{q^{\circ}}$ étant la fraction convergente qui précède $\frac{p}{q}$ et qui est donnée par le développement de celle-ci en fraction continue. Il faudra donc que $p^{\circ}-\alpha q^{\circ}$ soit plus grand que $p-\alpha q$, ou que $\frac{p^{\circ}-\alpha q^{\circ}}{p-\alpha q}$ soit plus grande que l'unité; mais d'ailleurs cette quantité peut être négative ou positive.

Soit d'abord $\frac{p^\circ - \alpha q^\circ}{p - \alpha q} = -y$, on en déduira $\alpha = \frac{py + p^\circ}{qy + q^\circ}$; donc, à cause de $y$ positif et plus grand que l'unité, $\frac{p^\circ}{q^\circ}$ et $\frac{p}{q}$ seront deux fractions consécutives convergentes vers $\alpha$, et $y$ sera le quotient-complet qui répond à la seconde.

En second lieu, soit $\frac{p^\circ - \alpha q^\circ}{p - \alpha q} = +y$, on aura $\alpha = \frac{py - p^\circ}{qy - q^\circ}$; mais il faut subdiviser ce cas en deux autres, selon que $y$ est $> 2$ ou $< 2$.

Si l'on a $y > 2$, on fera $y = 1 + z$, $z$ étant $> 1$, et on aura $\alpha = \frac{pz + p - p^\circ}{qz + q - q^\circ}$; donc $\frac{p - p^\circ}{q - q^\circ}$, $\frac{p}{q}$ seront encore deux fractions consécutives convergentes vers $\alpha$, et $z$ sera le quotient-complet qui répond à la dernière.

Dans ces premiers cas, qui présentent déjà une grande latitude, il est donc prouvé, d'une manière directe et fort simple, que $\frac{p}{q}$ est une fraction convergente vers la racine $\alpha$.

Il reste à examiner le dernier cas où l'on a $y < 2$. Soit alors $y = 1 + \frac{1}{z}$, $z$ étant toujours $> 1$, on aura

$$\alpha = \frac{(p - p^\circ)z + p}{(q - q^\circ)z + q} = \frac{(p - p^\circ)(z+1) + p^\circ}{(q - q^\circ)(z+1) + q^\circ};$$

donc $\frac{p^\circ}{q^\circ}$, $\frac{p - p^\circ}{q - q^\circ}$ seront deux fractions consécutives convergentes vers $\alpha$ (1), et le quotient-complet qui répond à la dernière sera $z + 1$, quantité plus grande que 2.

Il faudroit que le quotient fût seulement 1 plus une fraction, pour que $\frac{p}{q}$ fût la fraction convergente qui suit $\frac{p - p^\circ}{q - q^\circ}$; et puis-

(1) On suppose $p - p^\circ > p^\circ$, et en effet le développement de $\frac{p}{q}$ en fraction continue donne une suite de quotiens dont le dernier peut être supposé à volonté plus grand que l'unité ou égal à l'unité. Or si on le prend plus grand que l'unité, $p$ ne sera pas moindre que $2p^\circ + p^{\circ\circ}$, et ainsi on aura $p - p^\circ > p^\circ$.

qu'on a $z+1>2$, il s'ensuit que dans ce dernier cas $\frac{p}{q}$ ne peut plus être une fraction convergente vers $\alpha$; mais au moins puisque $\frac{p-p^\circ}{q-q^\circ}$ en est une, et que la différence entre $\frac{p}{q}$ et $\frac{p-p^\circ}{q-q^\circ}$ n'est que $\frac{1}{q(q-q^\circ)}$, on voit que $\frac{p}{q}$ est toujours une valeur fort approchée de la racine $\alpha$.

Soit $p-p^\circ=\pi$, $q-q^\circ=\varphi$, nous pourrons représenter par $\frac{p^\circ}{q^\circ}$, $\frac{\pi}{\varphi}$, $\frac{\pi'}{\varphi'}$, trois fractions consécutives convergentes vers $\alpha$; et parce que $q$ tombe entre $\varphi$ et $\varphi'$, il est clair qu'on aura (n°. 8) $p-\alpha q>\pi-\alpha\varphi$.

Mais en faisant $t=\pi$, $u=\varphi$, il faut qu'on ait $F(\pi,\varphi)>F(p,q)$, puisque celle-ci est un *minimum;* donc il y aura dans la valeur de $F(\pi,\varphi)$ quelqu'autre facteur $\pi-\alpha'\varphi$ plus grand que le facteur correspondant $p-\alpha' q$.

Or de ce que $\frac{\pi-\alpha'\varphi}{p-\alpha' q}$ est plus grand que l'unité, et peut être d'ailleurs positif ou négatif, on conclura comme ci-dessus que $\frac{p}{q}$ est une fraction convergente vers $\alpha'$, ou qu'au moins on a $\alpha'=\frac{(p-\pi)(z+1)+\pi}{(q-\varphi)(z+1)+\varphi}$, $z$ étant positif et $>1$; de-là résulte, en substituant les valeurs de $\pi$ et $\varphi$,

$$\alpha'=\frac{p^\circ(z+1)+p-p^\circ}{q^\circ(z+1)+q-q^\circ}=\frac{p^\circ z+p}{q^\circ z+q}=\frac{p^\circ(z+\mu^\circ)+p^{\circ\circ}}{q^\circ(z+\mu^\circ)+q^{\circ\circ}},$$

(car on suppose toujours $p=\mu^\circ p^\circ+p^{\circ\circ}$). Donc $\frac{p^{\circ\circ}}{q^{\circ\circ}}$, $\frac{p^\circ}{q^\circ}$ seront deux fractions consécutives convergentes vers $\alpha'$, et la fraction suivante sera $\frac{p^\circ(k+\mu^\circ)+p^{\circ\circ}}{q^\circ(k+\mu^\circ)+q^{\circ\circ}}$ ou $\frac{p^\circ k+p}{q^\circ k+q}$, $k$ étant l'entier compris dans $z$. Et puisque $q$ tombe entre $q^\circ$ et $q^\circ k+q$, il s'ensuit qu'on aura $p^\circ-\alpha' q^\circ<p-\alpha' q$.

Le même raisonnement s'applique aux autres racines $\alpha''$, $\alpha'''$, &c. et même aux quantités $\mathcal{C}$, $\mathcal{C}'$, $\mathcal{C}''$, &c.; il en résulte pour conclusion

générale, que la fraction $\frac{p}{q}$, qui répond au *minimum* de la fonction proposée, doit être comprise parmi les fractions convergentes vers l'une des racines $\alpha$, $\alpha'$, $\alpha''$, &c., ou vers l'une des quantités $\zeta$, $\zeta'$, $\zeta''$, &c. Car si elle n'y est pas comprise, il faudra que les conditions suivantes soient réunies.

1°. Que la quantité $\frac{p^\circ-\alpha q^\circ}{p-\alpha q}$ relative à une racine déterminée $\alpha$, soit comprise entre $+1$ et $+2$.

2°. Que toutes les quantités analogues $\frac{p^\circ-\alpha' q^\circ}{p-\alpha' q}$, $\frac{p^\circ-\alpha'' q^\circ}{p-\alpha'' q}$, &c. $\frac{p^\circ-\zeta q^\circ}{p-\zeta q}$, $\frac{p^\circ-\zeta' q^\circ}{p-\zeta' q}$, &c. relatives aux autres racines, soient plus petites que l'unité.

Mais cela posé, il paroît impossible que la quantité $\frac{F(p^\circ, q^\circ)}{F(p, q)}$ qui est composée du produit de tous les facteurs

$$\frac{p^\circ-\alpha q^\circ}{p-\alpha q},\ \frac{p^\circ-\alpha' q^\circ}{p-\alpha' q},\ \frac{p^\circ-\alpha'' q^\circ}{p-\alpha'' q} \ldots\ldots \frac{(p^\circ-\zeta q^\circ)^2+\gamma^2 q^{\circ 2}}{(p-\zeta q)^2+\gamma^2 q^2}, \text{ \&c.}$$

soit plus grande que l'unité, comme elle doit l'être, si $F(p, q)$ est un *minimum*.

En effet, puisque la différence entre $\frac{p}{q}$ et $\frac{p^\circ}{q^\circ}$ n'est que $\frac{1}{q q^\circ}$, et que $\frac{p^\circ}{q^\circ}$ est une fraction convergente vers $\alpha$, il suffit que parmi les racines $\alpha'$, $\alpha''$, &c. et les quantités $\zeta$, $\zeta'$, &c. il y en ait une ou d'un signe contraire de $\alpha$, ou dont la différence avec $\alpha$ soit sensiblement plus grande que $\frac{1}{q q^\circ}$; alors si $\alpha'$ est cette racine, le facteur $\frac{p^\circ-\alpha' q^\circ}{p-\alpha' q}$ sera à-peu-près $\frac{q^\circ}{q}$ et ainsi sera moindre que $\frac{1}{2}$; et si $\zeta$ est une quantité assez différente de $\alpha$, le facteur $\frac{(p^\circ-\zeta q^\circ)^2+\gamma^2 q^{\circ 2}}{(p-\zeta q)^2+\gamma^2 q^2}$ se réduira encore à très-peu-près à $\left(\frac{q^\circ}{q}\right)^2$ et sera par conséquent plus petit que $\frac{1}{4}$. Donc dans la valeur de $\frac{F(p^\circ, q^\circ)}{F(p, q)}$ il n'y auroit qu'un facteur plus grand que l'unité, mais moindre que 2; tandis

que tous les autres facteurs seroient plus petits qne l'unité, et que parmi ceux-ci il s'en trouveroit au moins un plus petit que $\frac{1}{2}$, ou même plus petit que $\frac{1}{4}$; donc cette quantité $\frac{F(p°, q°)}{F(p, q)}$ seroit plus petite que l'unité, ce qui est contraire à la supposition faite que $F(p, q)$ est un *minimum*. Donc enfin (1) la fraction $\frac{p}{q}$ est toujours une fraction convergente vers l'une des quantités $\alpha$, $\alpha'$, $\alpha''$... $\mathcal{C}$, $\mathcal{C}'$... &c.

(123) La condition qu'on vient de démontrer, ne détermine point encore le *minimum* qu'on cherche, elle indique senlement un ordre de quantités parmi lesquelles il faut chercher la fraction $\frac{p}{q}$ propre à donner ce *minimum*. Voici en conséquence le procédé qu'il faut suivre.

Développez en fraction continne successivement chacune des racines réelles $\alpha$ de l'équation $ax^n + bx^{n-1} + \ldots + k = 0$.

Développez de même chacune des parties réelles $\mathcal{C}$ des racines imaginaires de la même équation.

Prenez successivement pour $\frac{p}{q}$ toutes les fractions convergentes qui résultent de ces diverses opérations, et substituez les valeurs de $p$ et $q$ dans la fonction proposée. Vous aurez autant de résultats qui chacun dans son genre sont une sorte de *minimum*; le plus petit de tous ces résultats, ou le *minimum minimorum*, sera donc celui qu'il s'agissoit de déterminer.

REMARQUE I.

(124) Si la racine réelle $\alpha$, ou la partie réelle $\mathcal{C}$ d'une racine imaginaire est négative, on fera son développement en fraction continue, comme si elle étoit positive; mais ensuite on affectera

---

(1) On trouve cette proposition dans les additions à l'Algèbre d'Euler, n°. 28, mais le savant auteur n'est point entré dans le détail de la démonstration. On trouve également la même proposition démontrée, pour le cas où le *minimum* est 1, dans les Mém. de Berlin an. 1768; mais la démonstration est difficile à suivre, et il y a quelque différence dans l'énoncé, en ce qui concerne les quantités $\mathcal{C}$, $\mathcal{C}'$, &c.

chaque fraction convergente du signe — avant de la prendre pour $\frac{p}{q}$.

Ici se présente la question de savoir lequel des deux termes $p$ et $q$ sera pris négativement. Cette question est facile à résoudre : si l'exposant $n$ de l'équation proposée est un nombre pair, il est indifférent de faire porter le signe — sur l'un ou sur l'autre des deux termes $p$ et $q$, et la quantité $ap^n+bp^{n-1}q+$ &c. restera absolument la même. Si au contraire l'exposant $n$ est impair, la quantité $ap^n+bp^{n-1}q+$ &c. conservera la même valeur, mais changera de signe, lorsqu'au lieu de prendre $p$ positif et $q$ négatif, on prendra $p$ négatif et $q$ positif; ou en général lorsqu'on changera à-la-fois le signe de $p$ et celui de $q$.

De-là on voit que dans le cas de $n$ impair, l'équation $ap^n+bp^{n-1}q\ldots+kq^n=+H$, est toujours résoluble en même temps que l'équation $ap^n+bp^{n-1}q\ldots+kq^n=-H$.

REMARQUE II.

(125) Si on développe en fraction continue chaque racine $\alpha$, par la méthode exposée ci-dessus (n°. 100), on pourra se dispenser de calculer la valeur de $F(p,q)$ pour chaque fraction convergente $\frac{p}{q}$; en effet la transformée qui répond à la fraction $\frac{p}{q}$ étant $Az^n+Bz^{n-1}+$ &c. $=0$, le premier coefficient $A$ de cette transformée sera précisément la valeur de $F(p,q)$; donc il suffira de jeter les yeux sur le premier terme de chaque transformée pour avoir le *minimum* demandé.

La même chose auroit lieu à l'égard des quantités $\zeta$, si on faisoit leur développement au moyen de l'équation dont elles sont des racines réelles. Mais comme cette équation est pour l'ordinaire d'un degré trop élevé, il conviendra mieux de faire ce développement par le moyen d'une valeur approchée de $\zeta$, et on substituera au lieu de $\frac{p}{q}$, les fractions convergentes qui en résultent (n°. 114). D'ailleurs on va voir que le développement de ces quantités ne doit être prolongé que jusqu'à une certaine limite.

REMARQUE III.

(126) Les opérations indiquées sont les mêmes, soit que le *minimum* soit déjà déterminé, comme il l'est quand on se propose de

de résoudre l'équation $at^n + bt^{n-1}u + ct^{n-2}u^2 \ldots . + ku^n = \pm 1$, soit qu'on cherche simplement quelle est la moindre valeur dont le premier membre de cette équation est susceptible. Dans le premier cas, on sent bien que le problême ne sera pas toujours possible. Dans le second, il n'y a autre chose à faire que de chercher dans plusieurs séries de nombres connus quel est le plus petit.

Mais dans les deux cas, comme l'opération du développement s'étend à l'infini, et que passé le second degré on ne connoît aucune loi à laquelle soient assujettis les quotiens et les transformées successives, il est clair qu'on n'aura déterminé le *minimum* de la fonction $at^n + bt^{n-1}u \ldots + ku^n$ que dans l'hypothèse que $t$ et $u$ n'excèdent pas les plus grands termes des fractions convergentes calculées. On ne pourra donc assurer qu'un *minimum* pareil ou même plus petit (s'il n'est pas déjà $\pm 1$) ne puisse avoir lieu au moyen des fractions convergentes ultérieures dont les termes sont plus grands. En effet, on ne voit rien qui empêche que même avec de très-grandes valeurs de $p$ et $q$, la fonction $ap^n + bp^{n-1}q +$ &c. ne se réduise à l'unité ou à un nombre fort petit; de sorte qu'à cet égard il ne paroît pas qu'on puisse assigner de limite.

Nous observerons cependant que cette grandeur indéfinie des nombres $p$ et $q$ ne peut concerner les fractions convergentes qui résultent du développement de la partie réelle $\mathsf{6}$ d'une racine imaginaire $\mathsf{6} + \gamma\sqrt{-1}$. Car un facteur tel que $(p - \mathsf{6}q)^2 + \gamma^2 q^2$ ne peut diminuer que jusqu'à un certain point, savoir, tant que la diminution de la partie $(p - \mathsf{6}q)^2$ est plus considérable que l'augmentation de l'autre partie $\gamma^2 q^2$, mais bientôt après ces facteurs doivent augmenter rapidement. On voit par cette raison, qu'il n'est pas nécessaire de chercher les équations dont $\mathsf{6}$, $\mathsf{6}'$, &c, sont les racines, et qu'on peut se contenter, comme nous l'avons déjà dit, d'une valeur approchée de ces quantités.

(127) Supposons que $\frac{p}{q}$ soit une fraction convergente assez approchée de la racine $\alpha$, pour que la différence $\frac{p}{q} - \alpha$ soit beaucoup plus petite que la différence entre la racine $\alpha$ et chacune des autres racines ou parties de racines $\alpha', \alpha'' \ldots \mathsf{6}, \mathsf{6}'$ &c., alors si l'on fait pour abréger,

$$L = (\alpha - \alpha')(\alpha - \alpha'') \ldots . \left(\overline{\alpha - \beta}^2 + \gamma^2\right)\left(\overline{\alpha - \beta'}^2 + \gamma'^2\right)^2 \text{ \&c.}$$

on aura à très-peu-près $F(p, q) = aq^{n-1}(p - \alpha q)L$. Soit $z$ le quotient-complet qui répond à la fraction convergente $\frac{p}{q}$, on aura $p - \alpha q = \pm \frac{1}{qz + q^\circ}$; donc $F(p, q) = \pm aL. \frac{q^{n-2}}{z + \frac{q^\circ}{q}}$.

Dans cette formule, $aL$ étant une quantité constante, on voit que pour que $F(p,q)$ soit un nombre donné, il faut que le quotient $z$ soit en général proportionnel à $q^{n-2}$.

Ainsi, par exemple, si on veut que $F(p, q)$ se réduise à $\pm 1$, comme cela est nécessaire dans les équations que nous nous sommes proposées, il faut qu'on ait $z = aL q^{n-2}$ à-peu-près. Telle est la grandeur des qnotiens auxquels on reconnoîtra les fractions convergentes qui satisfont à la condition du *minimum* $F(p,q) = \pm 1$. Cette formule sera sur-tont utile, si le développement d'une racine se fait non par la méthode des transformées successives, mais par le moyen d'une valenr approchée de cette racine (n°. 112).

A mesure que l'opération du développement avance, la valenr de $q$ augmente, et par conséquent celle de $z$ (car on suppose ici $n > 2$), de sorte qu'il devient de moins en moins probable qu'on trouvera le quotient $z$ nécessaire pour le *minimum*. Cependant si la racine $\alpha$ est très-peu différente d'une ou de plusieurs autres racines $\alpha'$, $\alpha''$, &c. ou des quantités $\beta$, $\beta'$, &c., alors la limite $L$ pourra être extrêmement petite, et il ne faudra plus un quotient aussi considérable $z$ pour répondre au *minimum* de $F(p, q)$. Cette remarque s'accorde avec les propriétés que nous avons déjà exposées (n$^{os}$. 109 et 110).

Supposons en second lieu que $\frac{p}{q}$ soit l'une des fractions convergentes vers la quantité $\beta$; snpposons en même temps que la différence entre $\frac{p}{q}$ et $\beta$ soit beauconp plus petite que $\gamma$, et aussi beaucoup plus petite qu'aucune des quantités $\alpha, \alpha', \alpha'' \ldots \beta', \beta''$ &c. Cela posé, si l'on fait pour abréger,

$$\Lambda = (\beta - \alpha)(\beta - \alpha')(\beta' - \alpha'') \ldots [(\beta - \beta')^2 + \gamma'^2] \text{ \&c.},$$

on aura à très-peu-près $F(p,q) = a q^n \gamma^2 \Lambda$. Donc si on veut que

$F(p,q) = \pm 1$, il faudra qu'on ait $q^n = \pm \frac{1}{a\gamma^n \Lambda}$; ainsi $q$ ne peut surpasser $\sqrt[n]{\frac{1}{a\gamma^n \Lambda}}$; d'où l'on voit que le *minimum* $\pm 1$ ne pourra avoir lieu, à l'aide des racines imaginaires, que dans des cas très-limités, lorsque $\gamma$ ou $\Lambda$ seront très-petits, c'est-à-dire lorsqu'il y aura des racines presqu'égales. En même temps on a la limite du dénominateur $q$, au-delà de laquelle il est inutile de prolonger le développement de la quantité $\zeta$, ainsi que l'essai des fractions convergentes qui en résultent.

Nous avons déjà donné, dans le paragraphe précédent, des exemples de la résolution des équations indéterminées homogènes dont le second membre est $\pm 1$, nous nous contenterons d'ajouter un nouvel exemple où une solution est donnée par la racine réelle, et une par les racines imaginaires.

EXEMPLE.

(128) Soit proposé de trouver le *minimum* de la fonction

$$7t^3 - 110t^2u + 565tu^2 - 941u^3,$$

je considère l'équation $7x^3 - 110x^2 + 565x - 941 = 0$, et je trouve, après quelques essais, qu'elle a une racine réelle entre 3 et 4, et deux racines imaginaires peu différentes entr'elles. Voici le développement de la racine réelle en fraction continue :

| | | |
|---|---|---|
| $7x^3 - 110x^2 + 565x - 941 = 0$ | 3 | 1 : 0 |
| $-47z^3 + 94z^2 - 47z + 7 = 0$ | 1 | 3 : 1 |
| $7z^3 - 47z - 47 = 0$ | 2 | 4 : 1 |
| $-85z^3 + 37z^2 + 42z + 7 = 0$ | 1 | 11 : 3 |
| $z^3 - 139z^2 - 218z - 85 = 0$ | 140 | 15 : 4 |
| $-11005z^3 + 19662z^2 + 281z + 1 = 0$ | 1 | 2111 : 563 |
| $8939z^3 + 6590z^2 - 13353z - 11005 = 0$ | 1 | 2126 : 567 |
| $-8829z^3 + 26644z^2 + 33407z + 8939 = 0$ | 4 | 4237 : 1130 |
| $3807z^3 - 177233z^2 - 79304z - 8829 = 0$ | 46 | 19074 : 5087 |
| $-8123689z^3 + 7782096z^2 + 348133z + 3807 = 0$ | 1 | 877404 : 235132 |
| $10347z^3 - 8458742z^2 - 16588971z - 8123689 = 0$ | 819 | 896478 : 240219 |
| &c. | 2 | &c. |
| | 6 | |
| | 2 | |
| | &c. | |

On voit, par les premiers termes des transformées, que le *minimum* $+1$ a lieu lorsque $t=15$ et $u=4$, de sorte que ces valeurs satisfont à l'équation

$$7t^3-110t^2u+565tu^2-941u^3=1.$$

Dans le reste de l'opération, on ne trouve plus de transformées dont le premier terme ait pour coefficient 1, et ainsi on est certain que la première racine ne fournit plus d'autre solution de l'équation précédente, à moins de supposer le nombre $u$ beaucoup plus grand que $819\times240219$; mais par cette grandeur même, il paroît bien peu probable que l'opération prolongée fournisse de nouvelles valeurs de $t$ et $u$. Il reste à développer en fraction continue la partie réelle des racines imaginaires. Or comme l'équation n'est que du troisième degré, si on appelle $\alpha$ la racine réelle dont nous venons de trouver des valeurs approchées, la partie réelle $\zeta$ des racines imaginaires sera $\zeta=\frac{110}{14}-\frac{1}{2}\alpha$; substituant la valeur connue de $\alpha$, et développant le résultat en fraction continue, on aura les quotiens et les fractions convergentes vers $\zeta$ comme il suit:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Quotiens..... | 5, | 1, | 55, | 1, | 2, | 2, | 1, | 3 |
| Fract. converg. | $\frac{1}{0}$, | $\frac{5}{1}$, | $\frac{6}{1}$, | $\frac{335}{56}$, | $\frac{341}{57}$, | &c. | | |

Or en prenant successivement pour $\frac{t}{u}$ ces diverses fractions convergentes, on trouve que les valeurs $t=6$, $u=1$, donnent encore le *minimum* $+1$, et fournissent ainsi une seconde solution de l'équation indéterminée $7t^3-110t^2u$ &c. $=1$. Il seroit inutile de prendre pour $\frac{t}{u}$ d'autres fractions convergentes, parce que la limite trouvée ci-dessus $q=\sqrt[n]{\frac{1}{a\gamma^2\Lambda}}$ donne à très-peu-près $q=1$.

# SECONDE PARTIE.

## *PROPRIÉTÉS GÉNÉRALES DES NOMBRES.*

### §. I. *THÉORÈMES sur les Nombres premiers.*

(129) THÉORÈME. *Si* c *est un nombre premier, et* N *un nombre quelconque non divisible par* c, *je dis que la quantité* $N^{c-1}-1$ *sera divisible par* c, *de sorte qu'on aura* $\frac{N^{c-1}-1}{c}=$ *entier* $=$ e (1).

Soit $x$ un nombre entier quelconque, si on considère la formule connue

$$(1+x)^c=1+cx+\frac{c.c-1}{1.2}x^2+\frac{c.c-1.c-2}{1.2.3}x^3+\ldots\ldots+cx^{c-1}+x^c,$$

il est aisé de voir que tous les termes de cette suite, à l'exception du premier et du dernier, sont divisibles par $c$. En effet, soit $M$ le coefficient de $x^m$, on aura $M=\frac{c.c-1.c-2\ldots.c-m+1}{1.\ 2\ .\ 3\ldots\ldots\ m}$, ou $M.1.2.3\ldots m=c.c-1.c-2\ldots c-m+1$; et puisque le second membre est divisible par $c$, il faut que le premier le soit aussi. Mais l'exposant $m$, dans les termes dont il s'agit, ne surpasse pas $c-1$; donc $c$, qui est supposé un nombre premier, ne peut diviser le produit $1.2.3\ldots m$, donc il divise nécessairement $M$ pour toute valeur de $m$ depuis 1 jusqu'à $c-1$. Donc la quantité $(1+x)^c-1-x^c$ est divisible par $c$, quel que soit l'entier $x$.

Soit maintenant $1+x=N$, la quantité précédente deviendra $N^c-(N-1)^c-1$; et puisqu'elle est divisible par $c$, si on omet les

(1) Ce théorème, l'un des principaux de la théorie des nombres, est dû à Fermat; il a été démontré par Euler dans divers endroits des Mémoires de Pétersbourg, et notamment dans le Tome I des *Novi commentarii.*

multiples de $c$, on aura $N^c - 1 = (N-1)^c$, ou $N^c - N = (N-1)^c - (N-1)$. Mais en mettant $N-1$ à la place de $N$, et négligeant toujours les multiples de $c$, on aura semblablement $(N-1)^c - (N-1) = (N-2)^c - (N-2)$. Continuant ainsi de restes égaux en restes égaux, on parviendra nécessairement au reste $(N-N)^c - (N-N)$, lequel est évidemment zéro. Donc tous les restes précédens le sont; donc $N^c - N$ est divisible par $c$.

Mais $N^c - N$ est le produit de $N$ par $N^{c-1} - 1$, donc puisque $N$ est supposé non-divisible par $c$, il faudra que $N^{c-1} - 1$ soit divisible par $c$; *ce qu'il falloit démontrer.*

*Corollaire.* Lorsque $c$ est un nombre premier, on satisfera à l'équation $\frac{x^{c-1}-1}{c} = e$, en prenant pour $x$ un nombre quelconque non-divisible par $c$. Donc si on considère seulement les valeurs de $x$ positives et moindres que $c$, ces valeurs seront les nombres successifs $1, 2, 3, 4 \ldots c-1$; et si on considère les valeurs ou solutions comprises entre $-\frac{1}{2}c$ et $+\frac{1}{2}c$, ces valeurs ou solutions seront $\pm 1, \pm 2, \pm 3 \ldots \pm\left(\frac{c-1}{2}\right)$. Dans les deux cas, les solutions de l'équation dont il s'agit, sont au nombre de $c-1$ égal à l'exposant de $x$.

(130) THÉORÈME. *Si* n *est un nombre premier, le produit* $1.2.3\ldots(n-1)$ *augmenté d'une unité, sera divisible par* n.

En effet, il résulte de la théorie des différences qu'on a, quel que soit $m$, l'équation

$$1.2.3\ldots m = m^m - \frac{m}{1}(m-1)^m + \frac{m.m-1}{1.2}(m-2)^m - \frac{m.m-1.m-2}{1.2.3}(m-3)^m + \&c.$$

Si l'on fait $m = n-1$, et qu'on néglige les multiples de $n$, on aura, suivant le théorême précédent,

$$m^m = 1, \quad (m-1)^m = 1, \quad (m-2)^m = 1, \quad \&c.$$

Donc le produit $1.2.3\ldots m$, en faisant les mêmes omissions, se réduit à $1 - m + \frac{m.m-1}{1.2} - \frac{m.m-1.m-2}{1.2.3} + \&c.$, le nombre des termes de cette suite étant $m$. Mais ces $m$ termes composent la

puissance développée $(1-1)^m$ moins son dernier terme, qui est $+1$, parce que $m$ est pair. Donc la somme des termes en question $=(1-1)^m-1=-1$. Donc la quantité $1.2.3.....(n-1)+1$ est divisible par $n$.

(131) Ce théorême, dont Waring fait mention dans ses *Meditationes Algebraicæ*; et dont il attribue la découverte à Jean Wilson, a été démontré pour la première fois par Lagrange dans les Mémoires de Berlin, année 1771, et ensuite par Euler dans ses *Opuscula Analytica, Tom. I.* Il est sur-tout remarquable, en ce qu'il n'a lieu que lorsque $n$ est un nombre premier. En effet, si $n$ est composé de deux facteurs quelconques inégaux $a$ et $b$, ces deux facteurs se trouveront nécessairement tous deux parmi les nombres $1, 2, 3, \ldots (n-1)$, et la quantité $1.2.3\ldots(n-1)+1$ divisée par $n$, laissera pour reste $+1$. La même chose auroit lieu, quand même $n$ seroit égal au produit des deux facteurs égaux $a\times a$; car alors $a$ et $2a$ se trouveroient dans la suite $1, 2, 3\ldots n-1$. Donc le produit de ces nombres seroit divisible par $a^2$ ou $n$, et ce produit, augmenté d'une unité, laisseroit pour reste 1.

On peut déduire de-là une règle générale et infaillible, pour reconnoître si un nombre donné $n$ est premier ou s'il ne l'est pas. Pour cela, il faut ajouter une unité au produit $1.2.3\ldots(n-1)$; si la somme est divisible par $n$, le nombre $n$ sera premier; si elle ne l'est pas, le nombre $n$ sera composé. Mais quoique cette règle soit très-belle *in abstracto*, elle ne peut guère être utile dans la pratique, attendu la grandeur énorme à laquelle s'élève bientôt le produit $1.2.3\ldots(n-1)$.

Observons que les nombres $n-1, n-2, n-3$, &c. considérés comme restes de la division par $n$, sont équivalens aux restes $-1, -2, -3$, &c.; d'ailleurs $n$ étant supposé impair, le nombre des facteurs $1, 2, 3\ldots n-1$ sera pair. Donc le produit $1.2.3\ldots(n-1)$, divisé par $n$, laissera le même reste que $\pm 1^2.2^2.3^2\ldots\left(\frac{n-1}{2}\right)^2$, le signe ambigu étant $+$ lorsque $n$ est de la forme $4k+1$, et $-$ lorsqu'il est de la forme $4k-1$.

Donc 1°. si le nombre premier $n$ est de la forme $4k+1$, la quan-

tité $\left(1.2.3\ldots\frac{n-1}{2}\right)^2+1$ sera divisible par $n$. On connoît donc ainsi une somme de deux quarrés $a^2+1$ dont $n$ doit être diviseur.

2°. Si le nombre premier $n$ est de la forme $4k-1$, la quantité $\left(1.2.3\ldots\frac{n-1}{2}\right)^2-1$ sera divisible par $n$, et par conséquent $n$ doit diviser l'une ou l'autre des deux quantités $1.2.3\ldots\left(\frac{n-1}{2}\right)+1$, $1.2.3\ldots\left(\frac{n-1}{2}\right)-1$.

(132) Lemme. *Soit* c *un nombre premier, et* P *un polynome du degré* m, *savoir* $P=\alpha x^m+\beta x^{m-1}+\gamma x^{m-2}\ldots+\omega$; *je dis qu'il ne peut y avoir plus de* m *valeurs de* x, *comprises entre* $+\frac{1}{2}c$ *et* $-\frac{1}{2}c$, *qui rendent ce polynome divisible par* c.

Car soit $k$ une première valeur de $x$ qui rende $P$ divisible par $c$, on pourra faire $P=(x-k)P'+\mathcal{A}c$, et on aura pour $P'$ un polynome en $x$ du degré $m-1$. Soit $k'$ une seconde valeur de $x$ qui rende $P$ divisible par $c$, il faudra que cette valeur rende $(x-k)P'$ divisible par $c$. Mais le facteur $x-k$, qui devient $k'-k$, ne peut être divisible par $c$, puisque $k$ et $k'$ sont supposés chacun plus petits que $\frac{1}{2}c$; donc $P$ ne pourra être divisible une seconde fois par $c$, à moins que $P'$ ne le soit. Le polynome $P$ du degré $m$ n'admet par conséquent qu'une solution de plus que le polynome $P'$ du degré $m-1$; donc il ne peut y avoir au plus que $m$ valeurs différentes de $x$, comprises entre $\frac{1}{2}c$ et $-\frac{1}{2}c$, qui rendent $P$ divisible par $c$.

Nous regarderons comme *solution* ou *racine* de l'équation $\frac{P}{c}=e$, toute valeur de $x$, comprise entre $+\frac{1}{2}c$ et $-\frac{1}{2}c$, qui rend le premier membre égal à un entier. Le nombre de ces solutions, qu'on pourroit prendre aussi entre o et $c$, ne doit jamais surpasser l'exposant $m$, comme il vient d'être démontré; mais d'après une solution telle que $x=k$, on peut faire plus généralement $x=k+cz$, et toutes les valeurs de $x$ renfermées dans cette formule, satisferont à l'équation $\frac{P}{c}=e$.

(133)

(133) THÉORÈME. *Soit toujours* c *un nombre premier*, *et* P *un polynome du degré* m, *lequel soit diviseur du binome* $x^{c-1}-1$; *je dis qu'il y aura toujours* m *valeurs de* x, *comprises entre* $+\frac{1}{2}c$ *et* $-\frac{1}{2}c$, *qui rendent ce polynome divisible par* c.

Car soit $x^{c-1}-1=PQ$, $Q$ étant un autre polynome du degré $c-1-m$. Puisqu'il y a $c-1$ valeurs de $x$, savoir $\pm 1, \pm 2, \pm 3 \ldots \pm \frac{c-1}{2}$, qui rendent le premier membre divisible par $c$, il faut que chacune de ces valeurs rende $P$ ou $Q$ divisible par $c$. Parmi ces $c-1$ valeurs, il ne peut y en avoir plus de $m$ qui rendent $P$ divisible par $c$, parce que $P$ n'est que du degré $m$; il ne peut non plus y en avoir moins de $m$, car alors il y auroit plus de $c-1-m$ valeurs de $x$ qui rendroient $Q$ divisible par $c$; ce qui est impossible, puisque $Q$ n'est que du degré $c-1-m$. Donc le nombre de valeurs de $x$ qui rendent $P$ divisible par $c$, et qui sont comprises entre $+\frac{1}{2}c$ et $-\frac{1}{2}c$, est précisément $m$.

*Remarque*. La même proposition auroit lieu, si $P$ étoit diviseur de $x^{c-1}-1+cR$, $R$ étant un polynome d'un degré quelconque moindre que $c$.

(134) THÉORÈME. *Si le nombre premier* c *est diviseur de* $x^2+N$, N *étant un nombre donné positif ou négatif*, *je dis que la quantité* $(-N)^{\frac{c-1}{2}}-1$ *doit être divisible par* c; *et réciproquement si cette condition est remplie*, *il existera un nombre* x (*moindre que* $\frac{1}{2}c$) *tel que* $x^2+N$ *sera divisible par* c. (*On excepte le cas de* $c=2$, *et celui où* N *est divisible par* c.)

Car 1°. si $c$ est diviseur de $x^2+N$, on aura, en omettant les multiples de $c$, $x^2=-N$; donc $x^{c-1}-1=(-N)^{\frac{c-1}{2}}-1$. Le premier membre est divisible par $c$, donc le second doit l'être également.

2°. Si on suppose que $(-N)^{\frac{c-1}{2}}-1$ soit divisible par $c$, je fais cette quantité $=cr$, ce qui donnera $x^{c-1}-1-cr=x^{c-1}-(-N)^{\frac{c-1}{2}}$. Mais si l'on fait, pour un moment, $c-1=2b$, $-N=M$, le second membre devient $x^{2b}-M^b$, lequel est divisible par $x^2-M$ ou $x^2+N$. Donc $x^2+N$ divise également le premier membre

Aa

$x^{c-1}-1-cr$. Donc (n°. 133) il y a nécessairement deux valeurs de $x$, moindres que $\frac{1}{2}c$, qui rendent $x^2+N$ divisible par $c$; ces deux valeurs n'en font proprement qu'une, parce qu'elles ne diffèrent que par leur signe.

*Remarque.* Nous avons démontré que $N$ étant un nombre quelconque, et $c$ un nombre premier qui ne divise pas $N$, la quantité $N^{c-1}-1$ est toujours divisible par $c$; cette quantité est le produit des deux facteurs $N^{\frac{c-1}{2}}+1$, $N^{\frac{c-1}{2}}-1$; il faut donc que l'un ou l'autre de ces deux facteurs soit divisible par $c$; d'où nous conclurons que la quantité $N^{\frac{c-1}{2}}$ divisée par $c$, laissera toujours le reste $+1$ ou le reste $-1$.

(135) *Comme les quantités analogues à* $\mathrm{N}^{\frac{c-1}{2}}$ *se rencontreront fréquemment dans le cours de nos recherches, nous emploierons le caractère abrégé* $\left(\frac{\mathrm{N}}{\mathrm{c}}\right)$ *pour exprimer le reste que donne* $\mathrm{N}^{\frac{c-1}{2}}$ *divisé par* c; *reste qui, suivant ce qu'on vient de voir, ne peut être que* $+1$ *ou* $-1$.

Dans l'expression $\left(\frac{N}{c}\right)$ le nombre $N$ est un nombre quelconque positif ou négatif, mais $c$ est toujours un nombre premier, 2 excepté.

## §. II. *Recherche de la forme qui convient aux diviseurs de la formule* $t^2+au^2$.

(136) Dans la formule $t^2+au^2$, nous regarderons $a$ comme un nombre donné positif ou négatif, et nous supposerons que $t$ et $u$ sont deux indéterminées auxquelles on peut attribuer toutes les valeurs possibles, en nombres entiers positifs ou négatifs, mais avec la condition essentielle que $t$ et $u$ soient premiers entr'eux. En effet, sans cette condition il n'y auroit aucun nombre qui ne pût diviser la formule $t^2+au^2$, et il n'y auroit par conséquent aucune forme particulière qui caractérisât les diviseurs de cette formule. Cela posé, on voit que pour une même valeur de $a$, la formule $t^2+au^2$ représentera une infinité de nombres différens, et il s'agit d'examiner la nature des diviseurs de cette formule.

Soit $p$ un diviseur quelconque de la formule $t^2+au^2$, et soit en conséquence $t^2+au^2=Pp$ : je dis d'abord que les nombres $u$ et $p$ sont premiers entr'eux : car si $u^2$ et $p$ avoient un commun diviseur $\theta$, il est clair que $\theta$ diviseroit $Pp-au^2$ ou $t^2$, et qu'ainsi $t$ et $u$ auroient un commun diviseur, ce qui est contre la supposition. Puis donc que $p$ et $u$ sont premiers entr'eux, on pourra (n°. 13) trouver deux nombres $y$ et $q$ tels qu'on ait $t=py+qu$. Substituant cette valeur dans l'équation $t^2+au^2=Pp$ et divisant tout par $p$, on aura

$$py^2+2qyu+\left(\frac{q^2+a}{p}\right)u^2=P.$$

Mais puisque $u$ n'a aucun diviseur commun avec $p$, cette équation ne peut subsister à moins que $\frac{q^2+a}{p}$ ne soit un entier. Donc le nombre $p$ qui divise la formule $t^2+au^2$, divisera également la formule moins générale $x^2+a$, en faisant $x=q$.

(137) Non-seulement la formule à deux indéterminées $t^2+au^2$, n'a pas d'autres diviseurs que la formule à une seule indéterminée

$t^2+a$ ou $x^2+a$; mais à cet égard la formule $\mathcal{A}t^2+Btu+Cu^2$, où $\mathcal{A}$, $B$, $C$ sont des nombres donnés, n'est pas plus générale que les deux premières. En effet si on multiplie la dernière par $4\mathcal{A}$, et qu'on fasse $2\mathcal{A}t+Bu=x$, $4\mathcal{A}C-B^2=a$, le produit sera $x^2+au^2$. Donc les diviseurs de la formule $\mathcal{A}t^2+Btu+Cu^2$ sont les mêmes que ceux de la formule plus simple $x^2+au^2$, ou même $x^2+a$, $a$ étant égale à la quantité constante $4\mathcal{A}C-B^2$. Et quoiqu'on ait multiplié par $4\mathcal{A}$ la formule proposée, il n'y a pas même exception par rapport aux diviseurs qui ne seroient pas premiers à $\mathcal{A}$, car en faisant $x=B$, la formule $x^2+a$ devient $B^2+a$ ou $4\mathcal{A}C$; elle est par conséquent divisible par $\mathcal{A}$.

Soit toujours $p$ un diviseur quelconque de la formule $t^2+au^2$, et supposons que $\theta$, $\gamma$, $\delta$, &c. soient les nombres premiers qui divisent $p$, il faudra que chacun de ces nombres divise la formule $x^2+a$; ainsi, d'après le n°. 134 et la notation indiquée n°. 135, il faudra qu'on ait les équations

$$\left(\frac{-a}{\theta}\right)=1,\ \left(\frac{-a}{\gamma}\right)=1,\ \left(\frac{-a}{\delta}\right)=1,\ \&c.$$

Ces conditions seront suffisantes, au moins tant que $p$ et $a$ n'auront pas de commun diviseur.

(138) Revenons à la formule $py^2+2qyu+\left(\frac{q^2+a}{p}\right)u^2=P$, et puisque $\frac{q^2+a}{p}$ est un entier, faisons $\frac{q^2+a}{p}=r$, nous aurons

$$P=py^2+2qyu+ru^2.$$

Mais $P$ peut désigner pareillement un diviseur quelconque de la formule $t^2+au^2$; donc tout diviseur de cette formule indéterminée peut être représenté par la formule de même degré $py^2+2qyu+ru^2$, dans laquelle on a $pr-q^2=a$.

Et comme on est maître de supposer $u=1$, puisque la formule $t^2+a$ doit avoir les mêmes diviseurs que la formule $t^2+au^2$, il s'ensuit qu'on peut aussi représenter l'un quelconque de ces diviseurs par la formule $py^2+2qy+r$, où l'on a également $pr-q^2=a$. Cette forme est plus simple que la précédente; cependant nous préférerons celle-ci, parce que ses coefficiens peuvent toujours

être renfermés entre des limites connues et dépendantes du seul nombre $a$.

En effet, nous avons démontré (n°. 46) que la formule indéterminée $py^2+2qyu+ru^2$ peut toujours être transformée en une formule semblable, dans laquelle le coefficient moyen $2q$ n'excédera aucun des coefficiens extrêmes $p$, $r$, et où l'on aura toujours $pr-q^2=a$.

Supposons que cette réduction soit effectuée, et nous serons en droit de conclure, selon que $a$ est positif ou négatif,

1°. Que tout diviseur de la formule $t^2+cu^2$, où $c$ est un nombre positif, peut être représenté par la formule $py^2+2qyz+rz^2$ dans laquelle on a $pr-q^2=c$, $2q<p$ et $r$, et par conséquent $q<\sqrt{\frac{c}{3}}$.

2°. Que tout diviseur de la formule $t^2-cu^2$, peut être représenté par la formule $py^2+2qyz-rz^2$, où l'on a $pr+q^2=c$, $2q<p$ et $r$, et par conséquent $q<\sqrt{\frac{c}{5}}$.

(139) Dans les deux cas, il faut se souvenir que les indéterminées $y$ et $z$ doivent être des nombres premiers entr'eux, comme le sont les indéterminées $t$ et $u$ de la formule proposée $t^2\pm cu^2$. Avec cette condition, tout nombre $P$ renfermé dans la formule $py^2+2qyz\pm rz^2$ sera nécessairement diviseur de la formule $t^2\pm cu^2$.

Car supposons qu'on ait $P=p\alpha^2+2q\alpha\beta\pm r\beta^2$, et soit $\frac{\alpha^0}{\beta^0}$ la fraction convergente qui précède $\frac{\alpha}{\beta}$ dans le développement de celle-ci en fraction continue. Si à la place de $y$ et $z$ on met $\alpha y+\alpha^0 z$ et $\beta y+\beta^0 z$ dans la formule indéterminée $py^2+2qyz\pm rz^2$, le résultat sera (n°. 45) de la forme $Py^2+2Qyz+Rz^2$, où l'on aura $PR=Q^2\pm c$. Donc $P$ est diviseur de $Q^2\pm c$ ou de $t^2\pm cu^2$.

## §. III. *Application de la théorie précédente à diverses formules* $t^2+u^2$, $t^2+2u^2$, $t^2-2u^2$, *&c. Conséquences qui en résultent pour les formes générales des nombres premiers.*

(140) **Pour** avoir les diviseurs de la formule $t^2+u^2$, il faudra, suivant la méthode du §. précédent, faire $c=1$, $pr-q^2=1$, et $q<\sqrt{\frac{1}{3}}$; on aura donc $q=0$, $pr=1$, $p=r=1$, et le diviseur $py^2+2qyz+rz^2$ se réduit à $y^2+z^2$. Donc *tout diviseur de la formule* $t^2+u^2$, *composée de deux quarrés premiers entr'eux, est également la somme de deux quarrés premiers entr'eux.*

Ce théorême étant d'un très-grand usage dans la théorie des nombres, nous croyons devoir en donner une seconde démonstration fondée sur d'autres principes.

Soit $N$ un nombre quelconque qui divise la somme de deux quarrés premiers entr'eux $t^2+u^2$, on pourra supposer que les nombres $t$ et $u$ ne surpassent pas $\frac{1}{2}N$; car puisque $N$ divise $t^2+u^2$, il divisera également $(t-\alpha N)^2+(u-\beta N)^2$; or les nombres $\alpha$ et $\beta$ peuvent toujours être pris de manière que $t-\alpha N$ et $u-\beta N$ n'excèdent pas $\frac{1}{2}N$.

Cette préparation étant supposée faite, la quantité $t^2+u^2$ sera moindre que $\frac{1}{2}N^2$, ainsi en faisant $t^2+u^2=NN'$, on aura $N'<\frac{1}{2}N$.

Et d'abord si on avoit $N'=1$, le nombre $N$ seroit égal à $t^2+u^2$, et la proposition seroit vérifiée.

Soit donc $N'>1$; puisque $N'$ divise $t^2+u^2$, il divisera aussi $(t-\alpha N')^2+(u-\beta N')^2$; or on peut prendre $\alpha$ et $\beta$ de manière que $t-\alpha N'$ et $u-\beta N'$ n'excèdent pas $\frac{1}{2}N'$. Si l'on fait donc dans cette hypothèse

$$(t-\alpha N')^2+(u-\beta N')^2=N'N'',$$

on aura $N''<\frac{1}{2}N'$. Multipliant cette équation membre à membre par l'équation $t^2+u^2=NN'$, on trouvera que le produit peut être mis sous la forme

$$(t^2+u^2-\alpha N'-\beta N')^2+(\alpha N'-\beta N')^2=NN'^2N''.$$

Substituant dans le premier membre $NN'$ au lieu de $t^2+u^2$, et divisant tout par $N'^2$, on aura

$$(N'-\alpha-\mathcal{C})^2 + (\alpha-\mathcal{C})^2 = NN''.$$

Si dans ce nouveau résultat, on avoit $N''=1$, le nombre $N$ seroit égal à la somme de deux quarrés, et la proposition seroit démontrée.

Soit donc encore $N''>1$, alors, en suivant la même marche, on déduira du produit $NN''$ un nouveau produit $NN'''$ où l'on aura $N'''<\frac{1}{2}N''$, et qui sera exprimé pareillement par la somme de deux quarrés.

Mais la suite des nombres entiers $N$, $N'$, $N''$, $N'''$, &c. dont chacun est moindre que la moitié du précédent, ne sauroit aller à l'infini; on parviendra donc nécessairement à un terme égal à l'unité, et alors le nombre $N$ sera égal à la somme de deux quarrés. *Donc tout diviseur* &c.

(141) Revenons à la méthode générale, et proposons-nous de déterminer les diviseurs de la formule $t^2+2u^2$. On aura, dans ce cas, $c=2$, $pr-q^2=2$, $q<\sqrt{\frac{2}{3}}$; donc il faut faire encore $q=0$, ce qui donne $pr=2$, et par conséquent $p=1$, $r=2$. Donc le diviseur $py^2+2qyz+rz^2$ sera toujours de la forme $y^2+2z^2$ semblable à la formule dividende $t^2+2u^2$.

Soit encore la formule $t^2-2u^2$, dont nous représenterons un diviseur quelconque par $py^2+2qyz-rz^2$, on aura $c=2$, $pr+q^2=2$, $q<\sqrt{\frac{2}{3}}$. Il en résulte $q=0$ et $pr=2$, ce qui donne $p=1$, $r=2$, ou $p=2$, $r=1$. Donc tout diviseur de la formule $t^2-2u^2$ peut être représenté, soit par $y^2-2z^2$, soit par $2y^2-z^2$. Ces deux formes, au reste, se réduisent à une seule, car nous avons déjà observé qu'on a

$$y^2-2z^2=2(y-z)^2-(y-2z)^2.$$

On trouvera de la même manière, que la formule $t^2+3u^2$ ne peut avoir pour diviseur impair qu'un nombre de forme semblable $y^2+3z^2$, et aussi que la formule $t^2-5u^2$ ne peut avoir pour diviseur impair que l'une ou l'autre des deux formes $y^2-5z^2$, $5y^2-z^2$. Or il est aisé de voir que ces deux formes se réduisent encore à une seule, puisqu'on a

$$y^2-5z^2=5(y-2z)^2-(2y-5z)^2.$$

Donc en général *tout nombre compris dans l'une des formes* $t^2+u^2$, $t^2+2u^2$, $t^2-2u^2$, $t^2+3u^2$, $t^2-5u^2$, $t$ *et* $u$ *étant premiers entr'eux, ne peut avoir pour diviseur qu'un nombre de même forme. Il faut excepter seulement, à l'égard des deux dernières formules* $t^2+3u^2$, $t^2-5u^2$, *les diviseurs doubles d'un impair, lesquels ne pourroient être des formes* $y^2+3z^2$, $y^2-5z^2$.

Ces diverses formes, qui ont l'avantage de se reproduire dans leurs diviseurs, ne sont point incompatibles entr'elles; elles se trouvent au contraire réunies assez souvent, deux ou plusieurs, dans le même nombre. Ainsi on a $89=8^2+5^2=9^2+2.2^2$; $241=15^2+4^2=13^2+2.6^2=21^2-2.10^2=7^2+3.8^2=31^2-5.12^2$.

(142) C'est ici le lieu de développer quelques-unes des propriétés des nombres fondées sur la combinaison des quarrés pairs et impairs; et d'abord observons qu'un quarré pair $(2x)^2$ est toujours de la forme $4n$, et un quarré impair $(2x+1)^2$ de la forme $8n+1$. En effet on a $4x^2+4x+1=8\left(\frac{x^2+x}{2}\right)+1$; or $\frac{x^2+x}{2}$ est toujours un entier, et de plus, cet entier est un nombre triangulaire (1).

(1) Voici les différentes séries de nombres auxquels on a donné le nom de *nombres figurés :*

| | | |
|---|---|---|
| *A* | 1, 2, 3, 4, 5, 6 ....... | $n$ |
| *B* | 1, 3, 6, 10, 15, 21 ..... | $\frac{n.\overline{n+1}}{1.2}$ |
| *C* | 1, 4, 10, 20, 35, 56..... | $\frac{n.\overline{n+1}.\overline{n+2}}{1.2.3}$ |
| *D* | 1, 5, 15, 35, 70, 126 .... | $\frac{n.\overline{n+1}.\overline{n+2}.\overline{n+3}}{1.2.3.4}$ |
| &c. | &c., &c. | |

La première série *A* est celle des *nombres naturels* dont le terme général est $n$; la seconde série *B* est celle des *nombres triangulaires*, son terme général est $\frac{n.\overline{n+1}}{2}$. Si de ce terme général, qui est le $n^{ième}$ terme de la série *B*, on retranche le terme précédent de la même série, lequel est $\frac{\overline{n-1}.n}{2}$, le reste sera $n$, qui est le terme général ou $n^{ième}$ terme de la série *A*. Donc on formera le $n^{ième}$ terme

Puisque

Puisque $y^2$ et $z^2$ ne peuvent être que de l'une des formes $4n, 8n+1$, on établira immédiatement les trois propositions suivantes :

1°. *Tout nombre impair représenté par la formule* $y^2+z^2$ *est de la forme* $4n+1$.

2°. *Tout nombre impair représenté par la formule* $y^2+2z^2$ *est de l'une des formes* $8n+1$, $8n+3$.

3°. *Tout nombre impair représenté par la formule* $y^2-2z^2$ *est de l'une des formes* $8n+1$, $8n+7$.

De ces trois propositions résultent, par voie d'exclusion, ces trois autres :

4°. *Aucun nombre de la forme* $4n-1$ *ne peut être représenté par* $y^2+z^2$.

5°. *Aucun nombre des formes* $8n+5$, $8n+7$ *ne peut être représenté par* $y^2+2z^2$.

6°. *Aucun nombre des formes* $8n+3$, $8n+5$ *ne peut être représenté par* $y^2-2z^2$.

Cela posé, il sera facile de démontrer les quatre théorêmes suivans, qui sont d'une grande importance dans la théorie des nombres.

---

de la série *B*, en ajoutant le $(n-1)^{ième}$ terme de la même série avec le $n^{ième}$ de la série *A*.

La troisième série *C* est celle des *nombres pyramidaux*, dont le terme général est $\frac{n.\overline{n+1}.\overline{n+2}}{1.2.3}$ ; si de ce terme on retranche le précédent $\frac{\overline{n-1}.n.\overline{n+1}}{1.2.3}$, la différence sera $\frac{n.\overline{n+1}}{1.2}$, qui est le $n^{ième}$ terme de la série *B*. Donc on peut former la série *C* au moyen de la série *B*, comme on a formé celle-ci au moyen de la série *A*.

Il en est de même de la quatrième série *D*, qui est celle des *nombres triangulo-triangulaires*, et dont le terme général est $\frac{n.\overline{n+1}.\overline{n+2}.\overline{n+3}}{1.2.3.4}$, et ainsi des autres.

Les termes généraux que nous donnons ici comme définitions, et d'où nous déduisons la loi de formation successive, renferment toute la théorie des nombres figurés, et offrent immédiatement la démonstration d'une proposition générale dont Fermat fait mention dans ses notes sur Diophante, pag. 16, et qu'il regardoit comme une de ses principales découvertes.

(143) Théorème I. *Tout nombre premier* $4n+1$ *est la somme de deux quarrés.*

Soit ce nombre premier $c=4n+1$, on aura $x^{c-1}-1=x^{4n}-1$ $=(x^{2n}+1)(x^{2n}-1)$; donc (n°. 133) il y aura $2n$ valeurs de $x$, comprises entre $+\frac{1}{2}c$ et $-\frac{1}{2}c$, qui rendront $x^{2n}+1$ divisible par $c$. Mais $x^{2n}+1$ est la somme de deux quarrés premiers entr'eux, donc (n°. 140) son diviseur $c$ est également la somme de deux quarrés premiers; donc on pourra toujours supposer $c=y^2+z^2$. (1).

*Remarque.* La forme $4n+1$ renferme les deux formes $8n+1$, $8n+5$; donc tout nombre premier soit de la forme $8n+1$, soit de la forme $8n+5$, est la somme de deux quarrés.

(144) Théorème II. *Tout nombre premier* $8n+1$ *est à-la-fois des trois formes* $y^2+z^2$, $y^2+2z^2$, $y^2-2z^2$.

Soit ce nombre premier $c=8n+1$, on a déjà prouvé qu'il doit être de la forme $y^2+z^2$, ainsi il reste à démontrer qu'il est en même temps des deux autres formes $y^2+2z^2$, $y^2-2z^2$. Or on a $x^{c-1}-1=x^{8n}-1=(x^{4n}-1)(x^{4n}+1)$, donc (n°. 133) il y a $4n$ valeur de $x$, comprises entre $+\frac{1}{2}c$ et $-\frac{1}{2}c$, qui rendent le binome $x^{4n}+1$ divisible par $c$. Mais d'abord le binome $x^{4n}+1$ peut se mettre sous la forme $(x^{2n}-1)^2+2.x^{2n}$, laquelle est comprise dans la formule $t^2+2u^2$, $t$ et $u$ étant premiers entr'eux; donc son diviseur $c$ est de la forme $y^2+2z^2$.

En second lieu, le binome $x^{4n}+1$ peut aussi se mettre sous la forme $(x^{2n}+1)^2-2x^{2n}$, laquelle revient à $t^2-2u^2$; donc son diviseur $c$ doit être également de la forme $y^2-2z^2$.

Donc tout nombre premier $8n+1$ est à-la-fois des trois formes $y^2+z^2$, $y^2+2z^2$, $y^2-2z^2$. Et pour en donner un exemple, $73=8^2+3^2=1^2+2.6^2=9^2-2.2^2$.

---

(1) Il a été démontré (n°. 42) qu'on peut toujours satisfaire à l'équation $x^2-cy^2=-1$; il s'ensuit donc que $c$ est diviseur de $x^2+1$, et qu'ainsi $c$ est de la forme $y^2+z^2$. La même chose se tire encore du n°. 131, où l'on a trouvé une somme de deux quarrés $aa+1$ dont $c$ doit être diviseur.

(145) Théorème III. *Tout nombre premier* $8n+3$ *est de la forme* $y^2+2z^2$.

Car en faisant $c=8n+3$, et prenant en particulier $x=2$, la formule $x^{c-1}-1$ devient $2^{8n+2}-1=(2^{4n+1}-1)(2^{4n+1}+1)$; donc il faut que l'un de ces facteurs binomes soit divisible par $c$. Mais si le premier facteur, qui est de la forme $2t^2-u^2$, étoit divisible par $c$, le nombre $c$ lui-même seroit de la forme $2y^2-z^2$ ou $y^2-2z^2$, laquelle, comme on l'a vu n°. 142, ne peut convenir à aucun nombre $8n+3$. Donc $c$ divise nécessairement le second facteur $2.2^{4n}+1$, lequel est de la forme $t^2+2u^2$, donc $c$ est de la même forme $y^2+2z^2$. (1).

(146) Théorème IV. *Tout nombre premier* $8n+7$ *est de la forme* $y^2-2z^2$.

Car en faisant $c=8n+7$, et prenant encore $x=2$, on aura $x^{c-1}-1=(2^{4n+3}+1)(2^{4n+3}-1)$; le premier membre (n°. 129) doit être divisible par $c$, donc il faut que $c$ divise l'un des facteurs du second membre. Mais en doublant ces facteurs, et faisant $2^{2n+2}=k$, ils deviennent $k^2+2$, $k^2-2$; or si $c$ divisoit $k^2+2$, il seroit de la forme $y^2+2z^2$ laquelle (n°. 142) ne peut convenir à aucun nombre $8n+7$. Donc $c$ divise nécessairement l'autre facteur $k^2-2$, donc il est de la forme $y^2-2z^2$. (2).

Corollaire général.

(147) Il suit de ces quatre théorêmes, que les nombres premiers

---

(1) On a démontré ci-dessus, n°. 43, que $c$ étant un nombre premier $8n+3$, il est toujours possible de satisfaire à l'équation $x^2-cy^2=-2$: de-là il résulte fort directement que $c$ est diviseur de $x^2+2$, et qu'ainsi $c$ est de la forme $y^2+2z^2$.

(2) C'est encore ce qu'on peut déduire immédiatement de la proposition du n°. 44; car puisque, suivant cette proposition, l'équation $x^2-cy^2=2$ est toujours possible, il s'ensuit que $c$ divise $x^2-2$, et qu'ainsi $c$ est de la forme $y^2-2z^2$.

Ces quatre théorêmes, et quelques autres semblables, ont été découverts par Fermat; mais les démonstrations de ce savant ne nous ont point été transmises. Euler a démontré le premier et le second dans les nouveaux Comment. de Pétersburg; Lagrange a démontré les autres dans les Mém. de Berlin, ann. 1775.

impairs étant distribués en quatre classes ou espèces $8n+1$, $8n+3$, $8n+5$, $8n+7$, on peut établir les propriétés suivantes qui distinguent deux espèces de deux autres :

1°. *Les nombres premiers* $8n+1$, $8n+5$, *sont, exclusivement à tous autres, de la forme* $y^2+z^2$.

2°. *Les nombres premiers* $8n+1$, $8n+3$, *sont, exclusivement à tous autres, de la forme* $y^2+2z^2$.

3°. *Les nombres premiers* $8n+1$, $8n+7$, *sont, exclusivement à tous autres, de la forme* $y^2-2z^2$.

D'où l'on voit que la seule espèce $8n+1$, dans laquelle l'unité est comprise, réunit les trois propriétés, et que chacune des trois autres espèces ne jouit que d'une seule de ces mêmes propriétés.

A l'aide de ces théorêmes, il est facile d'évaluer l'expression $\left(\frac{2}{c}\right)$ selon les diverses formes du nombre premier $c$. On se souviendra que cette expression désigne le reste de $2^{\frac{c-1}{2}}$ divisé par $c$, reste qui ne peut être que $+1$ ou $-1$.

(148) Théorême V. *L'expression* $\left(\frac{2}{c}\right)$ *sera égale à* $+1$, *si le nombre premier* $c$ *est de forme* $8n+1$ *ou* $8n+7$; *elle sera égale à* $-1$, *si le nombre premier* $c$ *est de l'une des deux autres formes* $8n+3$, $8n+5$.

Car 1°. si $c$ est de l'une des formes $8n+1$, $8n+7$, on pourra faire $c=y^2-2z^2$; ou $2z^2=y^2-c$. Élevant chaque membre à la puissance $\frac{c-1}{2}$ et négligeant les multiples de $c$, on aura $2^{\frac{c-1}{2}}z^{c-1}=y^{c-1}$; mais en omettant ces mêmes multiples, on peut faire (n°. 129) $y^{c-1}=1$, $z^{c-1}=1$. Donc $2^{\frac{c-1}{2}}=1$, ou suivant notre notation abrégée $\left(\frac{2}{c}\right)=1$.

2°. Si $c$ est de la forme $8n+3$, on pourra faire $c=y^2+2z^2$, ou $2z^2=c-y^2$. Élevant chaque membre à la puissance $\frac{c-1}{2}$ et

observant que $\frac{c-1}{2}$ est impair, on aura, en négligeant toujours les multiples de $c$, $2^{\frac{c-1}{2}} z^{c-1} = -y^{c-1}$, ou $2^{\frac{c-1}{2}} = -1$, ou enfin $\left(\frac{2}{c}\right) = -1$.

3°. Si $c$ est de la forme $8n+5$, $c$ ne pourra être de la forme $y^2 - 2z^2$, donc $c$ ne pourra diviser un nombre de la forme $t^2 - 2u^2$. Mais si $c$ divisoit un nombre $t^2 - 2u^2$, on auroit (en vertu du n°. 134) $\left(\frac{2}{c}\right) = 1$; donc puisqu'on ne peut avoir $\left(\frac{2}{c}\right) = 1$, on aura nécessairement $\left(\frac{2}{c}\right) = -1$.

---

## §. IV. *Où l'on prouve que tout nombre entier est composé de quatre ou d'un moindre nombre de quarrés.*

Nous commencerons par démontrer la proposition suivante, qui n'est pas seulement subsidiaire pour l'objet que nous avons en vue, mais qui contient une propriété très-remarquable des nombres premiers.

(149) Théorème. *Étant donné un nombre premier* A *et deux autres nombres quelconques* B *et* C, *positifs ou négatifs, mais non divisibles par* A, *je dis qu'on peut toujours trouver deux nombres* t *et* u, *tels que la quantité* $t^2 - Bu^2 - C$ *soit divisible par* A. (Lagrange, Mém. de Berlin 1770.)

Car 1°. si l'on peut trouver un nombre $u$ tel que $Bu^2+C$ soit divisible par $A$, on prendra pour $t$ un multiple de $A$, et la formule $t^2-Bu^2-C$ sera divisible par $A$.

2°. S'il n'y a aucun nombre qui remplisse cette condition, faisons pour abréger $A=2a+1$, $Bu^2+C=V$, la quantité dont il s'agit $t^2-Bu^2-C$ ou $t^2-V$ étant un diviseur de $t^{2a}-V^a$, on pourra faire le quotient

$$t^{2a-2}+Vt^{2a-4}+V^2t^{2a-6}\ldots\ldots+V^{a-1}=P,$$

et on aura

$$(t^2-V)\,P=t^{2a}-V^a=t^{2a}-1-(V^a-1).$$

Soit $Q=V^a+1$, et en multipliant de part et d'autre par $Q$, on aura

$$(t^2-V)\,P\,Q=Q(t^{2a}-1)-(V^{2a}-1).$$

Mais d'après le théorême de Fermat (n°. 129), on sait que le second membre est divisible par $A$, pourvu que $t$ et $V$ soient premiers à $A$. Donc si, outre ces deux conditions, on peut faire en sorte que $A$ ne divise ni $P$ ni $Q$, on en conclura avec certitude que $t^2-V$ est divisible par $A$, ce qui est l'objet de notre démonstration.

Mais d'abord on a supposé que $V$ n'est jamais divisible par $A$; et pour que $t$ ne le soit pas, il suffit de prendre pour $t$ l'un des nombres 1, 2, 3.... $A-1$. Ainsi les deux premières conditions

se remplissent d'elles-mêmes, et il ne s'agit plus que de satisfaire aux deux autres, c'est-à-dire de faire en sorte que $A$ ne divise ni $P$ ni $Q$.

Or 1°. je remarque que la fonction $P$, considérée par rapport à l'indéterminée $t$, n'est que du degré $2a-2$ ou $A-3$; donc (n°. 132) il y a au plus $A-3$ valeurs de $t$, entre o et $A$, qui rendent cette fonction divisible par $A$. Donc il y a au moins deux valeurs de $t$, toujours entre o et $A$, qui rendront $P$ non divisible par $A$, et qui satisferont ainsi à la première condition.

2°. La quantité $Q=V^a+1=(Bu^2+C)^a+1$ étant développée, donne

$$Q=1+B^a u^{2a}+aB^{a-1}Cu^{2a-2}+\frac{a.a-1}{1.2}B^{a-2}C^2u^{2a-4}+\ \&c.$$
$$+C^a \quad +aBC^{a-1}u^2 \quad +\frac{a.a-1}{1.2}B^2C^{a-2}u^4+\ \&c.$$

Or il faut de deux choses l'une (n°. 134), ou que $C^a-1$ soit divisible par $A$, ou que $C_a+1$ le soit. Si le premier cas a lieu, ou en d'autres termes, si l'on a $\left(\frac{C}{A}\right)=1$, on pourra faire $u=0$, et la quantité $Q$ sera non-divisible par $A$. Ce cas, au reste, est évident par lui-même, puisqu'indépendamment du terme $Bu^2$ qu'on peut faire zéro ou multiple de $A$, la partie $t^2-C$ est divisible par $A$, en vertu de la condition $\left(\frac{C}{A}\right)=1$.

Si le second cas a lieu, ou si l'on a $\left(\frac{C}{A}\right)=-1$, alors en séparant dans $Q$ la partie $C^a+1$ qui est divisible par $A$, et divisant le reste par $u^2$, nous aurons le quotient

$$Q'=B^a u^{2a-2}+aB^{a-1}Cu^{2a-4}+\ldots\ldots+aBC^{a-1}.$$

Cette fonction, considérée par rapport à $u$, n'étant que du degré $2a-2$ ou $A-3$, il ne peut y avoir au plus que $A-3$ valeurs de $u$, qui rendent $Q'$ divisible par $A$; donc il y aura au moins deux valeurs de $u$ qui rendent $Q'$, et par conséquent $Q$ non divisible par $A$.

Donc il sera toujours possible de satisfaire aux conditions exi-

gées, et ainsi les nombres $t$ et $u$ sont toujours déterminables, de manière que la quantité $t^2 - Bu^2 - C$ soit divisible par le nombre premier $A$.

*Corollaire.* Si l'on fait $B = C = -1$, on conclura de cette proposition, que tout nombre premier $A$ est diviseur de la formule $t^2 + u^2 + 1$. C'est ce qu'Euler a démontré le premier dans le Tom. V des nouveaux Commentaires de Pétersbourg.

(150) LEMME. *Le produit d'une somme de quatre quarrés par une somme de quatre quarrés, est semblablement la somme de quatre quarrés.*

Il suffit, pour s'en assurer, de développer la formule suivante, qu'on trouvera être identique :

$$\begin{aligned}&(p^2+q^2+r^2+s^2)\,(p'^2+q'^2+r'^2+s'^2)\\ =\ &(pp'+qq'+rr'+ss')^2+(pq'-qp'+rs'-sr')^2\\ +\ &(pr'-qs'-rp'+sq')^2+(ps'+qr'-rq'-sp')^2.\end{aligned}$$

Dans cette formule, on peut changer à volonté le signe de chacune des lettres qui y entrent, ce qui donnera plusieurs manières de décomposer en quatre quarrés le produit dont il s'agit (1).

*Remarque.* Ce beau théorême d'algèbre est encore dû à Euler; il a été généralisé depuis par Lagrange dans les termes suivans : (Mémoires de Berlin, année 1770).

$$\begin{aligned}&(p^2-Bq^2-Cr^2+BCs^2)\,(p'^2-Bq'^2-Cr'^2+BCs'^2)\\ =\ &(pp'+Bqq'\pm Crr'\pm BCss')^2-B(pq'+p'q\pm Crs'\pm Cr's)^2\\ -\ &C(pr'-Bqs'\pm rp'\mp Bsq')^2+BC(qr'-ps'\pm sp'\mp rq')^2.\end{aligned}$$

(1) On peut s'assurer qu'il n'existe aucune formule semblable pour trois quarrés, c'est-à-dire que le produit d'une somme de trois quarrés par une somme de trois quarrés, ne peut pas être exprimé généralement par une somme de trois quarrés. Car si cela étoit possible, le produit $(1+1+1)\,(16+4+1)$, qui est 63, pourroit se décomposer en trois quarrés. Or cela n'a lieu (n°. 153) ni pour le nombre 63, ni pour aucun nombre $8n+7$.

Par la même raison, ou par l'exemple de $(1+4+2.4)\,(0+4+2.1)$, on démontreroit que le produit de deux formules telles que $p^2+q^2+2r^2$, $p'^2+q'^2+2r'^2$ ne peut généralement être égal à une formule semblable $x^2+y^2+2z^2$.

On

On voit par cette formule, que deux fonctions de la forme $x^2 - By^2 - Cz^2 + BCu^2$, $B$ et $C$ étant des coefficiens constans, donnent pour leur produit une fonction semblable. Donc un nombre quelconque de semblables fonctions multipliées entr'elles, donneroient pour leur produit une fonction semblable.

(151) Théorème. *Tout nombre premier* A *est de la forme* $p^2 + q^2 + r^2 + s^2$.

On a prouvé (n°. 149) qu'il existe toujours deux nombres $t$ et $u$, tels que $t^2 + u^2 + 1$ est divisible par $A$. Mais si à la place de $t$ et $u$ on met $t - A\alpha$ et $u - A\beta$, le résultat $(t - A\alpha)^2 + (u - A\beta)^2 + 1$ sera encore divisible par $A$; on peut donc supposer que les premières valeurs de $t$ et $u$ sont moindres que $\frac{1}{2}A$, ou qu'elles ont été rendues telles en en retranchant des multiples de $A$. Cela posé, si l'on fait

$$AA' = t^2 + u^2 + 1,$$

on aura $AA' < \frac{1}{4}A^2 + \frac{1}{4}A^2 + 1$, ou $A' < \frac{1}{2}A + \frac{1}{A}$.

Considérons plus généralement l'équation

$$AA' = p^2 + q^2 + r^2 + s^2,$$

dans laquelle chacun des nombres $p$, $q$, $r$, $s$ sera supposé moindre que $\frac{1}{2}A$, on aura $A'A < \frac{4}{4}A^2$, ou $A' < A$. Et d'abord si on avoit $A' = 1$, il est clair que $A$ seroit égal à la somme de quatre quarrés, et la proposition seroit démontrée.

Soit donc $A' > 1$, et parce que $A'$ est diviseur de $p^2 + q^2 + r^2 + s^2$, il sera aussi divisenr de la quantité $(p - \alpha A')^2 + (q - \beta A')^2 + (r - \gamma A')^2 + (s - \delta A')^2$, $\alpha$, $\beta$, $\gamma$, $\delta$ étant pris à volonté. Supposons qu'on prenne ces indéterminées de manière qu'aucun des termes $p - \alpha A'$, $q - \beta A'$, &c. n'excède $\frac{1}{2}A'$, alors si l'on fait

$$A'A'' = (p - \alpha A')^2 + (q - \beta A')^2 + (r - \gamma A')^2 + (s - \delta A')^2,$$

on aura $A'A'' < \frac{4}{4}A'A'$ ou $A'' < A'$. Maintenant si au moyen de la formule du n°. 150 on multiplie la valeur de $AA'$ par celle de $A'A''$, on trouvera pour produit une somme de quatre quarrés dont chacun est divisible par $A'A'$; de sorte qu'en divisant tout par $A'^2$, on aura

$$AA'' = (A - \alpha p - \beta q - \gamma r - \delta s)^2 + (\alpha q - \beta p + \gamma s - \delta r)^2$$
$$+ (\alpha r - \gamma p + \delta q - \beta s)^2 + (\alpha s - \delta p + \beta r - \gamma q)^2.$$

Cela posé, si on a $A''=1$, la proposition sera démontrée; mais si on a $A''>1$, on procédera de la même manière pour obtenir un nouveau produit $AA'''$ exprimé par quatre quarrés, et dans lequel on aura $A'''<A''$. Continuant ainsi la suite des entiers décroissans $A$, $A'$, $A''$. $A'''$, &c., on parviendra nécessairement à un terme égal à l'unité; donc alors le nombre premier $A$ sera exprimé par la somme de quatre quarrés.

(152) Théorème. *Un nombre quelconque est la somme de quatre ou d'un moindre nombre de quarrés* (1).

C'est une conséquence immédiate de la proposition qu'on vient de démontrer, et du lemme qui la précède; car un nombre quelconque étant le produit de plusieurs nombres premiers égaux ou inégaux, et chacun des facteurs étant de la forme $p^2+q^2+r^2+s^2$, si on multiplie deux facteurs entr'eux, puis le produit des deux par un troisième, puis le produit des trois par un quatrième, &c. jusqu'à ce que tous les facteurs soient employés, il est clair que les produits successifs seront toujours la somme de quatre quarrés. Donc le produit final, qui est le nombre proposé, sera aussi la somme de quatre quarrés, et pourra être représenté par $p^2+q^2+r^2+s^2$. Rien n'empêche d'ailleurs qu'un ou plusieurs des quarrés $p^2, q^2, r^2, s^2$ ne soient zéro; donc un nombre quelconque est égal à la somme de quatre ou d'un moindre nombre de quarrés.

(153) Il n'est point de nombre entier qui ne soit compris dans la formule $p^2+q^2+r^2+s^2$, mais ils peuvent, pour la plus grande partie, être représentés par la formule plus simple $p^2+q^2+r^2$. En général, on peut affirmer que *tout nombre impair est de la forme* $p^2+q^2+r^2$, *excepté seulement les nombres* $8n+7$.

On excepte les nombres $8n+7$, parce que si des trois termes $p, q, r$, deux sont pairs et le troisième impair, la formule $p^2+q^2+r^2$ sera de la forme $4n+1$, et si les trois nombres $p$, $q$, $r$ sont impairs, la formule $p^2+q^2+r^2$ sera de la forme $8n+3$. Donc aucun nombre $8n+7$ ne peut être la somme de trois quarrés.

(1) Lagrange est le premier qui ait donné la démonstration de ce beau théorême (Mém. de Berlin 1770) : cette démonstration a été ensuite beaucoup simplifiée par Euler dans les *Acta Petrop.* an. 1777.

Si dans la formule $p^2+q^2+r^2+s^2$ on suppose deux termes égaux, on aura une nouvelle formule $p^2+q^2+2r^2$, laquelle est encore très-générale; car on peut affirmer que *tout nombre impair, sans exception, est de la forme* $p^2+q^2+2r^2$.

Ces propositions seront mises ci-après dans un plus grand jour: observons quant à présent, que les deux formes $p^2+q^2+r^2$, $p^2+q^2+2r^2$ dont il est question dans ces théorêmes, ont entr'elles une telle relation, que le double de l'une reproduit l'autre. C'est ce qu'on voit par les formules

$$2(p^2+q^2+r^2)=(p+q)^2+(p-q)^2+2r^2$$
$$2(p^2+q^2+2r^2)=(p+q)^2+(p-q)^2+4r^2.$$

(154) La proposition que nous avons démontrée dans ce paragraphe, fait partie d'une propriété générale des nombres polygones découverte par Fermat, et dont nous ne pouvons nous dispenser de faire mention. Mais d'abord il faut, en faveur de quelques lecteurs, expliquer ce qu'on entend par nombres polygones.

Si on considère différentes progressions arithmétiques qui commencent toutes par l'unité, et dont les raisons soient successivement 1, 2, 3, 4, &c.; si ensuite, par l'addition des termes de chaque progression, on forme une suite correspondante, ces différentes suites composeront ce qu'on appelle *les nombres polygones*; elles sont comprises dans le tableau suivant:

| *Progressions arithmétiques.* | *Suites des nombres polygones.* |
|---|---|
| 1, 2, 3, 4, 5.......... $n$ | 1, 3, 6, 10, 15.......... $\frac{n.n+1}{2}$ |
| 1, 3, 5, 7, 9..... $2n-1$ | 1, 4, 9, 16, 25.............. $n^2$ |
| 1, 4, 7, 10, 13... $3n-2$ | 1, 5, 12, 22, 35...... $\frac{n(3n-1)}{2}$ |
| 1, 5, 9, 13, 17... $4n-3$ | 1, 6, 15, 28, 45....... $n(2n-1)$ |
| . | . |
| . | . |
| . | . |
| 1, $\alpha+1$, $2\alpha+1$,.. $n\alpha-\alpha+1$ | 1, $\alpha+2$, $3\alpha+3$, ... $\frac{n(n-1)}{2}\alpha+n$ |

La première suite 1, 3, 6, &c. est celle des nombres triangulaires, la seconde 1, 4, 9, &c. celle des quarrés, la troisième 1, 5, 12, &c. celle des nombres pentagones, et ainsi de suite.

Voici maintenant la proposition dont nous voulons parler, telle qu'elle est énoncée par Fermat dans une de ses notes sur Diophante, page 180.

« *Imo propositionem pulcherrimam et maxime generalem nos primi deteximus. Nempe omnem numerum vel esse triangulum vel ex duobus aut tribus triangulis compositum, esse quadratum vel ex duobus aut tribus quadratis compositum; esse pentagonum vel ex duobus tribus quatuor aut quinque pentagonis compositum et sic deinceps in infinitum in hexagonis, heptagonis et polygonis quibus libet, enuntianda videlicet pro numero angulorum generali et mirabili propositione. Ejus autem demonstrationem quæ ex multis variis et abstrusissimis numerorum mysteriis derivatur hic apponere non licet, opus enim et librum integrum huic operi destinare decrevimus et Arithmeticen hac in parte ultra veteres et notos terminos mirum in modum promovere* ».

Nous avons rapporté les propres expressions de l'auteur, parce que c'est sur-tout dans ce passage qu'on voit que Fermat s'occupoit d'un grand ouvrage sur les nombres, lequel devoit contenir, comme il le dit lui-même, *multa varia et abstrusissima numerorum mysteria*. Les Géomètres regretteront long-temps que ce savant illustre n'ait pas réalisé son projet, ou que du moins ses parens ou amis, devenus dépositaires de ses manuscrits, n'en aient pas fait part au public. On y auroit trouvé sans doute, outre les démonstrations encore inconnues de plusieurs de ses théorêmes, des méthodes dignes de la sagacité de l'auteur; méthodes qui jointes aux découvertes postérieures, auroient contribué beaucoup à perfectionner cette partie très-difficile des sciences exactes.

Pour revenir à la proposition citée, si on considère qu'un moindre nombre de termes polygones est toujours contenu dans un plus grand, parce que zéro peut être mis à la place des termes qui manquent, et qu'en effet zéro est un terme de chaque suite des nombres polygones, on pourra énoncer plus brièvement la proposition dont il s'agit, en ces termes:

*Un nombre quelconque peut être formé par l'addition de trois nombres triangulaires; il peut être formé également par l'addition de quatre quarrés, par celle de cinq nombres pentagones, par celle de six hexagones, et ainsi à l'infini.*

(155) Soit donc $A$ un nombre donné, et $x, y, z$, &c. des nombres indéterminés, les différentes parties du théorême général pourront se détailler de la manière suivante :

1°. *Quel que soit le nombre donné* A, *on pourra toujours satisfaire à l'équation* $A = \frac{x^2+x}{2} + \frac{y^2+y}{2} + \frac{z^2+z}{2}$, *ou, ce qui revient au même, à l'équation* $8A+3 = (2x+1)^2 + (2y+1)^2 + (2z+1)^2$.

Cette première partie, si elle étoit démontrée, prouveroit que tout nombre de forme $8n+3$ est la somme de trois quarrés. Réciproquement, s'il étoit prouvé que tout nombre $8n+3$ est la somme de trois quarrés, il s'ensuivroit immédiatement que tout nombre entier est la somme de trois triangulaires.

2°. *Quel que soit le nombre donné* A, *on pourra satisfaire à l'équation* $A = x^2+y^2+z^2+u^2$.

Cette seconde partie a été démontrée ci-dessus d'une manière qui ne laisse rien à desirer : cependant il ne sera pas inutile de faire voir que la première partie a une liaison nécessaire avec la seconde. En effet, s'il étoit démontré qu'on peut toujours satisfaire à l'équation

$$8A+3 = x^2+y^2+z^2,$$

on tireroit de-là $8A+4 = x^2+y^2+z^2+1$. Mais les quatre quarrés du second membre ne pouvant être qu'impairs, les nombres $x+y$, $x-y$, $z+1$, $z-1$, seront pairs, et ainsi on aura en nombres entiers :

$$4A+2 = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+1}{2}\right)^2 + \left(\frac{z-1}{2}\right)^2.$$

ou pour abréger,

$$4A+2 = x'^2 + y'^2 + z'^2 + u'^2.$$

Or de ces quatre nouveaux quarrés deux doivent être pairs et deux impairs, sans quoi la somme ne pourroit être $4A+2$, on aura donc

$$4A+2 = 4a^2 + 4b^2 + (2c+1)^2 + (2d+1)^2;$$

d'où l'on déduira

$$2A+1 = (a+b)^2 + (a-b)^2 + (c+d+1)^2 + (c-d)^2.$$

Donc la première partie de la proposition générale, celle qui concerne les nombres triangulaires, étant supposée, il s'ensuit, comme conséquence immédiate, que tout nombre impair $2A+1$ est la somme de quatre quarrés. Mais si un nombre est la somme de quatre quarrés $m^2+n^2+p^2+q^2$, son double sera aussi une semblable somme, puisqu'on a

$$2(m^2+n^2+p^2+q^2)=(m+n)^2+(m-n)^2+(p+q)^2+(p-q)^2.$$

Donc un nombre quelconque est la somme de quatre quarrés.

On voit par-là que la première partie du théorême de Fermat renferme implicitement la seconde, et puisque celle-ci est démontrée rigoureusement par une autre voie, on doit regarder la première comme déjà pourvue d'un grand degré de probabilité.

3°. La troisième partie du théorême général donne

$$A=\frac{3x^2-x}{2}+\frac{3y^2-y}{2}+\frac{3z^2-z}{2}+\frac{3t^2-t}{2}+\frac{3u^2-u}{2},$$

ou

$$24A+5=(6x-1)^2+(6y-1)^2+(6z-1)^2+(6t-1)^2+(6u-1)^2;$$

de sorte que l'énoncé de cette proposition particulière revient à celui-ci : *tout nombre de la forme* $24A+5$ *est composé de cinq quarrés dont les côtés sont de la forme* $6m-1$.

4°. La quatrième partie donne

$$A=x(2x-1)+y(2y-1)+z(2z-1)+s(2s-1)+t(2t-1)+u(2u-1),$$

ou

$$8A+6=(4x-1)^2+(4y-1)^2+(4z-1)^2+(4s-1)^2+(4t-1)^2+(4u-1)^2.$$

Il faut donc que *tout nombre* $8A+6$ *se décompose en six quarrés dont les côtés sont de forme* $4m-1$.

En général, la proposition dont il s'agit se réduit toujours à la décomposition d'un nombre donné en quarrés, et toutes les propositions partielles sont contenues dans cette formule générale :

$$8\alpha A+(\alpha+2)(\alpha-2)^2=(2\alpha x-\alpha+2)^2+(2\alpha y-\alpha+2)^2+\&c,$$

le nombre des termes du second membre étant $\alpha+2$.

## §. V. *De la forme linéaire qui convient aux diviseurs de la formule* $a^n \pm 1$, $a$ *et* $n$ *étant des nombres donnés.*

(156) Il ne seroit pas plus général de considérer la formule $a^n \pm b^n$, $a$ et $b$ étant des nombres premiers entr'eux ; car si cette formule est divisible par le nombre premier $p$, on pourra toujours faire $a = bx + py$, et il faudra que $x^n \pm 1$ soit aussi divisible par $p$. Cela posé, nous examinerons successivement les deux formules $a^n + 1$, $a^n - 1$.

Soit proposé d'abord de trouver la condition nécessaire pour que le nombre premier $p$ divise la formule $a^n + 1$.

Quel que soit $p$, on peut toujours supposer $p = 2nx + \varpi$, $x$ étant une indéterminée et $\varpi$ un nombre positif moindre que $2n$. On aura donc, en rejetant les multiples de $p$, $a^n = -1$ ; on aura aussi, par le théorême de Fermat, et parce que $a$ ne sauroit être divisible par $p$, $a^{p-1} = +1$, ou $a^{2nx+\varpi-1} = 1$. Mais à cause de $a^n = -1$, on a $a^{2nx} = 1$, et ainsi l'équation précédente devient $a^{\varpi-1} = 1$ ; de sorte que nous avons à satisfaire aux deux conditions

$$a^n = -1 , \quad a^{\varpi-1} = 1.$$

La seconde sera remplie d'elle-même, si on a $\varpi = 1$, et alors la forme du diviseur deviendra $p = 2nx + 1$.

Si on a $\varpi > 1$, soit $\omega$ le plus grand commun diviseur de $n$ et de $\varpi - 1$, on pourra faire $n = n'\omega$, et $\varpi - 1 = \varpi'\omega$, ce qui donnera

$$a^{n'\omega} = -1 , \quad a^{\varpi'\omega} = 1.$$

Mais puisque $n'$ et $\varpi'$ sont premiers entr'eux, on pourra toujours trouver deux nombres entiers $f$ et $g$, tels que $fn' - g\varpi' = 1$. De-là je tire $(-1)^f = a^{fn'\omega} = a^{g\varpi'\omega+\omega} = a^\omega$, ou $a^\omega = (-1)^f$, et cette valeur étant substituée dans les deux équations $a^{n'\omega} = -1$, $a^{\varpi'\omega} = 1$, il en résulte les deux conditions

$$(-1)^{fn'} = -1 , \quad (-1)^{\varpi'f} = 1.$$

La première fait voir que $f$ et $n'$ doivent être des nombres impairs ; la seconde que $\pi'$ est un nombre pair. Celle-ci, au reste, renferme la première ; car si $\pi'$ est pair, il faudra bien, d'après l'équation $fn' = g\pi' + 1$, que $f$ et $n'$ soient impairs.

Cela posé, on aura $a^{\omega} = -1$, c'est-à-dire que $a^{\omega} + 1$ sera divisible par $p$.

Et comme les seules suppositions à faire sont celles de $\pi = 1$ et de $\pi > 1$, on peut établir le théorème général qui suit :

(157) *Tout nombre premier* p *qui divise la formule* $a^n + 1$, *doit être ou de la forme* $2nx + 1$, *ou tout au moins de la forme nécessaire pour diviser une autre formule* $a^{\omega} + 1$ *dans laquelle l'exposant* $\omega$ *est le quotient de* n *divisé par un nombre impair.*

Ce théorème s'appliquera de même aux diviseurs de $a\ + 1$, et fera connoître ainsi, de proche en proche, toutes les formes dont sont susceptibles les diviseurs de la formule proposée $a^n + 1$. Voici quelques corollaires principaux qu'on en déduit immédiatement, et qu'il suffira d'énoncer.

1°. Si l'exposant $n$ est un nombre premier impair, tout nombre premier qui divise la formule $a^n + 1$ doit être de la forme $2nx + 1$, ou au moins il divisera $a + 1$.

2°. Si l'exposant $n$ est une puissance de 2, la formule $a^n + 1$ ne pourra avoir pour diviseur que les nombres premiers compris dans la forme $2nx + 1$.

Ainsi si l'on veut chercher les diviseurs premiers de $2^{32} + 1 = 4\,294\,967\,297$, ils doivent être contenus dans la formule $64x + 1$; on essaiera donc successivement 193, 257, 449, 577, 641. La division réussit par 641, et on trouve le quotient 6700 417. Pour trouver les diviseurs de celui-ci, il faut essayer de même tous les nombres premiers de la forme $64x + 1$, plus grands que 641, et moindres que $2588 = \sqrt{6700417}$ ; ce sont 769, 1153, 1217, 1409, 1601, 2113. Et comme aucun de ces nombres ne divise 6700 417, on en conclura, avec assurance, que 6700 417 est un nombre premier.

3°. Si on a $n = \lambda\nu$, $\lambda$ étant un terme de la progression 2, 4, 8, 16,

16, &c., et $\nu$ un nombre premier, le diviseur premier de la formule $a^n+1$, sera de la forme $2nx+1$, ou tout au moins il divisera la formule $a^\lambda+1$, et alors il sera de la forme $2\lambda x+1$.

4°. Si on a $n=\mu\nu$, $\mu$ et $\nu$ étant deux nombres premiers impairs, le diviseur premier de la formule $a^n+1$ sera de la forme $2nx+1$, ou bien il divisera la formule $a^\mu+1$ et sera de la forme $2\mu x+1$, ou bien il divisera la formule $a^\nu+1$ et sera de la forme $2\nu x+1$, ou enfin il divisera la formule $a+1$. Ces cas ne s'excluent pas mutuellement; car, par exemple, il est clair que le nombre premier qui divise la formule $a+1$, divisera toutes les autres formules $a^\nu+1$, $a^\mu+1$, &c., et de même le nombre premier qui divise $a^\nu+1$, divisera nécessairement $a^n+1$.

(158) Il est inutile d'étendre ces corollaires à un plus grand nombre de cas. Observons seulement que lorsqu'il s'agira de trouver les diviseurs d'une formule proposée $a^n+1$, on cherchera successivement ceux de toutes les formules inférieures $a^\omega+1$, en commençant par celles où l'exposant de $a$ est le plus petit, et il ne restera plus à chercher, d'après la forme $2nx+1$, que les diviseurs qui ne divisent aucune des formules inférieures à $a^n+1$.

On observera encore que lorsque $n$ est un nombre impair, la formule $a^n+1$, multipliée par $a$, devient de la forme $x^2+a$, elle ne peut donc avoir pour diviseurs que les nombres premiers qui divisent $x^2+a$. Cette condition servira à exclure la moitié des nombres premiers renfermés dans la formule $2nx+1$; mais pour cet effet, il faut consulter ce qu'on démontrera ci-après sur les diviseurs de $x^2+a$. On peut voir dès-à-présent que si $a$ étoit 2, les diviseurs premiers de $x^2+2$ ne peuvent être que des formes $8m+1$, $8m+3$; d'où il arrive que les deux autres formes générales $8m+5$, $8m+7$ sont exclues, et ne diviseront jamais la formule $2^n+1$, $n$ étant impair. Une semblable exclusion aura également lieu pour d'autres valeurs de $a$.

### EXEMPLE.

(159) Proposons-nous de trouver tous les diviseurs du nombre 549 755 813 889 $= 2^{39}+1 = A$.

Je considère d'abord les formules inférieures $2^{13}+1$, $2^{3}+1$, $2^{1}+1$; la dernière donne 3 pour diviseur de toutes les formules précédentes.

La formule $2^{3}+1=9$, ne donne encore que 3 pour diviseur premier; elle apprend de plus que $A$ sera divisible par 9.

La formule $2^{13}+1=8193=3.2731$, si elle a un autre diviseur que 3, ne peut en avoir que dans la forme $26x+1$; mais comme le moindre nombre premier compris dans la forme $26x+1$, est 53 déjà trop grand, puisqu'il excède la racine de 2731, il s'ensuit que 2731 est un nombre premier, et qu'ainsi $2^{13}+1$ n'a pas d'autres facteurs que 3 et 2731.

Cela posé, le nombre $A$ doit être divisible par 9.2731; si on le divise d'abord par 3.2731, qui est la même chose que $2^{13}+1$, le quotient sera $2^{26}-2^{13}+1$, ou 67 100 673, et celui-ci étant divisé par 3, on aura $A=3^{2}.2731 . 22\,366\,891$.

Il ne reste donc plus qu'à chercher les diviseurs du nombre $B=22\,366\,891$; ces diviseurs doivent être de la forme $78x+1$, et puisqu'ils doivent aussi diviser la formule $t^{2}+2$, ils ne peuvent être que de l'une des formes $8n+1$, $8n+3$. Mais la forme $78x+1$, en comprend quatre autres, selon que $x$ est égal à l'un des nombres $4y$, $4y+1$, $4y+2$, $4y+3$; ces quatre formes sont :

$$312y+1,\ 312y+79,\ 312y+157,\ 312y+235.$$

La seconde et la troisième doivent être exclues comme étant comprises dans $8n+7$ et $8n+5$; ainsi tout nombre premier qui divisera $B$ doit être renfermé dans l'une des deux formes

$$312y+1\ ,\quad 312y+235.$$

Les nombres premiers compris dans ces formes, et en même temps moindres que $\sqrt{B}$, qui est environ 4620, sont 313, 547, 859, 937, 1171, 1249, 1483, 1873, 2731, 3121, 3433, 4057, 4603. Si on essaie successivement ces treize nombres, ou seulement douze (car il est inutile d'essayer 2731), on trouvera qu'aucun d'eux ne divise $B$; d'où l'on conclura que 22 366 891 est un nombre premier.

Le nombre $B$ étant diviseur de $t^{2}+2$, doit être de la forme $p^{2}+2q^{2}$; si on veut réellement mettre $B$ sous cette forme, on le pourra sans tâtonnement à l'aide de la formule suivante :

$$\frac{4m^4-2m^2+1}{3}=\left(\frac{2m^2\pm 2m-1}{3}\right)^2+2\left(\frac{2m^2\mp m-1}{3}\right)^2.$$

Or on a $B=\frac{2^{26}-2^{13}+1}{3}$; donc si on fait $m=2^6$, on trouvera

$$B=(2773)^2+2(2709)^2.$$

(160) Venons maintenant à la seconde question, et proposons-nous de trouver la forme que doivent avoir les diviseurs premiers du nombre donné $a^n-1$.

Quel que soit le nombre premier $p$ qui divise cette formule, on peut le supposer de la forme $p=nx+\pi$, $\pi$ étant un nombre positif moindre que $n$. On aura donc, en rejetant les multiples de $p$, $a^n=1$, et $a^{p-1}=1$, d'où résulte $a^{\pi-1}=1$. Dans cette dernière équation, on ne peut supposer que $\pi=1$, ou $\pi>1$.

1°. Si on a $\pi=1$, la forme du diviseur est $p=nx+1$; elle restera ainsi tant que $n$ sera pair; mais si $n$ est impair, il faudra nécessairement que $x$ soit pair, et ainsi on aura $p=2nz+1$.

2°. Si on a $\pi>1$, soit $\omega$ le plus grand commun diviseur de $n$ et de $\pi-1$, ($\omega$ devant être 1 lorsqu'il n'y a pas d'autre mesure commune) on pourra toujours trouver deux entiers $f$ et $g$, tels que $fn-g(\pi-1)=\omega$. Or les deux équations $a^n=1$, $a^{\pi-1}=1$, donnent $1=a^{fn}=a^{g(\pi-1)+\omega}=a^\omega$, ou $a^\omega=1$, donc $p$ sera diviseur de $a^\omega-1$; et ici il n'y a aucune restriction à apporter au résultat $a^\omega=1$, parce que l'équation $a^\omega=1$ satisfait aux deux $a^n=1$, $a^{\pi-1}=1$.

Cela posé, toute la théorie des diviseurs de la quantité $a^n-1$ est comprise dans le théorème suivant.

(161) *Tout nombre premier* p *qui divise la formule* $a^n-1$, *doit être compris dans la forme* $p=nx+1$, *ou au moins doit être diviseur de la formule* $a^\omega-1$, *dans laquelle* $\omega$ *est un sous-multiple de* n.

Ajoutons que si $n$ est impair, auquel cas la forme $nx+1$ devient $2nz+1$, le diviseur $p$ doit encore être compris dans les formes qui conviennent aux diviseurs de la formule $x^2-a$.

Le même théorême s'appliquant à la formule $a^{\mu}-1$, ou à telle autre qui résulte immédiatement des diviseurs de $n$, on aura, par la combinaison des résultats, tous les diviseurs de la formule proposée. Voici quelques corollaires généraux qui en résultent.

1°. Si le nombre $n$ est premier, tous les diviseurs de la formule $a^n-1$ seront compris dans la forme $2nz+1$, il faut seulement en excepter ceux qui peuvent diviser $a-1$.

2°. Si le nombre $n$ est le produit de deux nombres premiers $\mu$ et $\nu$ (2 excepté), le diviseur premier $p$ de la formule $a^n-1$ sera de la forme $2nz+1$; ou bien il divisera $a^{\mu}-1$, et sera de la forme $2\mu z+1$; ou bien il divisera $a^{\nu}-1$ et sera de la forme $2\nu z+1$; ou enfin il divisera $a-1$ et sera de la forme $2z+1$, laquelle convient à tous les nombres premiers. En effet, lorsque $n$ est impair, il est évident que $a-1$ divise $a^n-1$; donc tout diviseur de la première quantité doit être diviseur de la seconde.

3°. Si le nombre $n$ est une puissance de 2, et qu'on fasse $\alpha=\frac{1}{2}n$, $\beta=\frac{1}{2}\alpha$, $\gamma=\frac{1}{2}\beta$, &c. le diviseur $p$ de la formule $a^n-1$ sera de la forme $nx+1$, ou bien il sera de la forme $\alpha x+1$ et divisera la formule $a^{\alpha}-1$, ou bien il sera de la forme $\beta x+1$ et divisera la formule $a^{\beta}-1$, ainsi de suite jusqu'à la forme $2x+1$ qui divisera la formule $a^2-1$.

## Exemple I.

(162) Pour avoir tous les diviseurs du nombre $A=2^{32}-1$, nous formerons le tableau suivant, où l'on voit la formule proposée et celles qui s'en déduisent, avec les formes correspondantes du diviseur :

$$\begin{array}{ll}
p=32x+1 \ldots\ldots & A=2^{32}-1=(2^{16}+1)B \\
p=16x+1 & B=2^{16}-1=(2^8+1)C \\
p=8x+1 & C=2^8-1=(2^4+1)D \\
p=4x+1 & D=2^4-1=(2^2+1)E \\
p=2x+1 & E=2^2-1=3
\end{array}$$

Le dernier nombre $E$, qui se réduit à 3, doit diviser tous les précédens, et d'abord on a $D=(2^2+1).3=3.5$; ensuite $C=(2^4+1)D=3.5.17$. Le nombre $B$ contient les mêmes diviseurs que $C$, et de plus $2^8+1=257$, lequel est un nombre premier.

Enfin $A$ est le produit de $B$ par $2^{16}+1=65537$. Or comme $2^{16}+1$ ne peut avoir aucun diviseur commun avec $B$ qui est $2^{16}-1$, il s'ensuit que $2^{16}+1$ ou 65537 ne peut avoir pour diviseur que des nombres premiers de la forme $32x+1$. Mais les nombres premiers contenus dans cette forme et moindres que $\sqrt{65537}$ sont 97 et 193, lesquels ne divisent point 65537. Donc 65537 est un nombre premier, donc le nombre $A$ décomposé en ses facteurs premiers $=3.5.17.257.65537$. Si on multiplie cette valeur par celle qu'on a trouvée (pag. 211) pour $2^{32}+1$, on aura la valeur décomposée de $2^{64}-1$.

EXEMPLE II.

(163) Soit encore proposé le nombre $A=2^{31}-1$; comme l'exposant 31 est un nombre premier, les diviseurs de $A$ ne pourront être que de la forme $62x+1$, et il n'y aura aucune exception, attendu que $a-1$ se réduit dans ce cas à $2-1=1$. Si l'on considère en même temps que le nombre $2A$ est de la forme $t^2-2$, et qu'en conséquence les diviseurs de $A$ doivent être de l'une des formes $8n+1$, $8n+7$, on trouvera, en combinant ces dernières formes avec la première $62x+1$, que tout diviseur premier de $A$ est nécessairement de l'une des formes $248z+1$, $248z+63$. Or Euler nous apprend (Mém. de Berlin, ann. 1772, pag. 36) qu'après avoir essayé tous les nombres premiers contenus dans ces formes, jusqu'à 46339, racine du nombre $A$, il n'en a trouvé aucun qui fût diviseur de $A$; d'où il faut conclure, conformément à une assertion de Fermat, que le nombre $2^{31}-1=2\,147\,483\,647$ est un nombre premier. C'est le plus grand de ceux qui aient été vérifiés jusqu'à présent.

Nous ne terminerons pas ce paragraphe, sans observer qu'Euler est auteur des principaux théorêmes qui y sont contenus. Voyez le Tom. I. des *Novi Comment. Petrop.*

## §. VI. *Théorème contenant une loi de réciprocité qui existe entre deux nombres premiers quelconques.*

(164) Nous avons vu (n°. 135) que si $m$ et $n$ sont deux nombres premiers quelconques (impairs et inégaux), les expressions abrégées $\left(\frac{m}{n}\right)$, $\left(\frac{n}{m}\right)$ représentent l'une le reste de $m^{\frac{n-1}{2}}$ divisé par $n$, l'autre le reste de $n^{\frac{m-1}{2}}$ divisé par $m$; on a prouvé en même temps que l'un et l'autre restes ne peuvent jamais être que $+1$ ou $-1$. Cela posé, il existe une telle relation entre les deux restes $\left(\frac{m}{n}\right)$, $\left(\frac{n}{m}\right)$, que l'un étant connu, l'autre est immédiatement déterminé. Voici le théorème général qui contient cette relation.

*Quels que soient les nombres premiers* m *et* n, *s'ils ne sont pas tous deux de la forme* $4x-1$, *on aura toujours* $\left(\frac{n}{m}\right)=\left(\frac{m}{n}\right)$, *et s'ils sont tous deux de la forme* $4x-1$, *on aura* $\left(\frac{n}{m}\right)=-\left(\frac{m}{n}\right)$. *Ces deux cas généraux sont compris dans la formule*

$$\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\cdot\left(\frac{m}{n}\right).$$

Pour développer les différens cas de ce théorême, il est nécessaire de distinguer, par des lettres particulières, les nombres premiers de la forme $4x+1$, et ceux de la forme $4x-1$. Nous désignerons dans le cours de cette démonstration, les premiers par les lettres $A$, $a$, $\alpha$; les seconds par les lettres $B$, $b$, $\mathfrak{b}$. Cela entendu, le théorême que nous venons d'énoncer renferme les huit cas suivans :

I. Si l'on a $\left(\frac{A}{a}\right)=+1$, il s'ensuit $\left(\frac{a}{A}\right)=+1$

II. Si l'on a $\left(\frac{A}{a}\right)=-1$, il s'ensuit $\left(\frac{a}{A}\right)=-1$

III. Si l'on a $\left(\frac{a}{b}\right) = +1$, il s'ensuit $\left(\frac{b}{a}\right) = +1$

IV. Si l'on a $\left(\frac{a}{b}\right) = -1$, il s'ensuit $\left(\frac{b}{a}\right) = -1$

V. Si l'on a $\left(\frac{b}{a}\right) = +1$, il s'ensuit $\left(\frac{a}{b}\right) = +1$

VI. Si l'on a $\left(\frac{b}{a}\right) = -1$, il s'ensuit $\left(\frac{a}{b}\right) = -1$

VII. Si l'on a $\left(\frac{B}{b}\right) = +1$, il s'ensuit $\left(\frac{b}{B}\right) = -1$

VIII. Si l'on a $\left(\frac{B}{b}\right) = -1$, il s'ensuit $\left(\frac{b}{B}\right) = +1$.

(165) Pour procéder à la démonstration de ces différens cas, j'observe d'abord que l'équation indéterminée $\mathcal{A}x^2+ay^2=bz^2$, ou plus généralement l'équation $(4f+1)x^2+(4g+1)y^2=(4h-1)z^2$ est impossible : car le premier membre (où l'on doit supposer $x$ et $y$ premiers entr'eux) est toujours de la forme $4k+1$ ou $4k+2$, tandis que le second membre est de la forme $4k$ ou $4k-1$. Mais on a démontré, n°. 27, que l'équation $\mathcal{A}x^2+ay^2=bz^2$ seroit résoluble, si on pouvoit trouver trois entiers $\lambda$, $\mu$, $\nu$ tels que $\frac{\mathcal{A}\lambda^2+a}{b}$, $\frac{a\mu^2-b}{\mathcal{A}}$, $\frac{\mathcal{A}\nu^2-b}{a}$ fussent des entiers. D'un autre côté, si $b$ est diviseur de $\mathcal{A}\lambda^2+a$, il le sera de $(\mathcal{A}\lambda)^2+a\mathcal{A}$, et ainsi en vertu du n°. 134 on aura $\left(\frac{-a\mathcal{A}}{b}\right)=1$; réciproquement si cette condition a lieu, $b$ sera diviseur de $t^2+a\mathcal{A}$, et faisant $t=\mathcal{A}\lambda+bu$, on aura $\mathcal{A}\lambda^2+a$ divisible par $b$. De-là on voit que l'équation $\mathcal{A}x^2+ay^2=bz^2$ seroit résoluble, si on pouvoit satisfaire aux trois conditions

$$\left(\frac{-a\mathcal{A}}{b}\right)=1,\quad \left(\frac{ab}{\mathcal{A}}\right)=1,\quad \left(\frac{\mathcal{A}b}{a}\right)=1.$$

Il faut donc que ces conditions soient incompatibles entr'elles, c'est ce qui va nous fournir la démonstration de plusieurs cas du théorême. Observons avant tout, 1°. que $N$ étant un nombre

quelconque, et $a$ un nombre premier $4n+1$, on a toujours $\left(\frac{-N}{a}\right)=\left(\frac{N}{a}\right)$, parce que $\frac{a-1}{2}$ étant alors un nombre pair, l'expression $(-N)^{\frac{a-1}{2}}$ est la même chose que $(N)^{\frac{a-1}{2}}$; au contraire $b$ étant un nombre premier de la forme $4n-1$, on a toujours $\left(\frac{-N}{b}\right)=-\left(\frac{N}{b}\right)$.

2°. Qu'une expression telle que $\left(\frac{MN}{c}\right)$, $c$ étant un nombre premier quelconque, est la même chose que le produit des deux $\left(\frac{M}{c}\right)\cdot\left(\frac{N}{c}\right)$. Car soit $\left(\frac{M}{c}\right)=\pi$ et $\left(\frac{N}{c}\right)=\varphi$, le sens de ces expressions indique assez qu'on peut faire $M^{\frac{c-1}{2}}=Pc+\pi, N^{\frac{c-1}{2}}=Qc+\varphi$, donc le reste de $(MN)^{\frac{c-1}{2}}$ divisé par $c$, est le même que celui de $(Pc+\pi)(Qc+\varphi)$, lequel est $\pi\varphi$; donc on a $\left(\frac{MN}{c}\right)=\left(\frac{M}{c}\right)\cdot\left(\frac{N}{c}\right)$. Le même résultat s'appliquera également à un plus grand nombre de facteurs. Il s'ensuit de ces observations, que les trois conditions mentionnées, qui ne peuvent avoir lieu à la fois, sont :

$$\left(\frac{a}{b}\right)\cdot\left(\frac{A}{b}\right)=-1,\quad \left(\frac{a}{A}\right)\cdot\left(\frac{b}{A}\right)=1,\quad \left(\frac{A}{a}\right)\cdot\left(\frac{b}{a}\right)=1.$$

*Démonstration des cas IV et V.*

(166) Soit d'abord $A=1$, la seconde condition aura lieu d'elle-même, et les deux autres seront $\left(\frac{a}{b}\right)=-1$, $\left(\frac{b}{a}\right)=1$. Celles-ci ne peuvent avoir lieu à-la-fois, donc

IV. Si l'on a $\left(\frac{a}{b}\right)=-1$, il s'ensuit $\left(\frac{b}{a}\right)=-1$

V. Si l'on a $\left(\frac{b}{a}\right)=+1$, il s'ensuit $\left(\frac{a}{b}\right)=+1$.

*Démonstration des cas I et II.*

Soient donnés les nombres $a$ et $A$, et supposons qu'on prenne un

un auxiliaire $b$, tel que $\left(\frac{b}{a}\right)=1$ et $\left(\frac{A}{b}\right)=-1$, on aura, suivant ce qui vient d'être démontré, $\left(\frac{a}{b}\right)=1$ et $\left(\frac{b}{A}\right)=-1$; alors des trois conditions ci-dessus la première est remplie d'elle-même, et les deux autres deviennent $\left(\frac{a}{A}\right)=-1$, $\left(\frac{A}{a}\right)=1$. Celles-ci ne peuvent avoir lieu en même temps, donc

I. Si l'on a $\left(\frac{A}{a}\right)=+1$, il s'ensuit $\left(\frac{a}{A}\right)=+1$

II. Si l'on a $\left(\frac{a}{A}\right)=-1$, il s'ensuit $\left(\frac{A}{a}\right)=-1$.

*Démonstration des cas III et VI.*

(167) Soient donnés les nombres $a$ et $b$, et soit pris l'auxiliaire $A$ tel que $\left(\frac{A}{a}\right)=-1$ et $\left(\frac{A}{b}\right)=-1$, il s'ensuivra, par les cas déjà démontrés $\left(\frac{a}{A}\right)=-1$, $\left(\frac{b}{A}\right)=-1$. Au moyen de ces valeurs, la seconde des conditions ci-dessus est remplie, et les deux autres sont $\left(\frac{a}{b}\right)=1$, $\left(\frac{b}{a}\right)=-1$; celles-ci ne peuvent avoir lieu à-la-fois, donc

III. Si l'on a $\left(\frac{a}{b}\right)=1$, il s'ensuit $\left(\frac{b}{a}\right)=1$

VI. Si l'on a $\left(\frac{b}{a}\right)=-1$, il s'ensuit $\left(\frac{a}{b}\right)=-1$.

(168) Il ne reste donc plus à démontrer que les cas VII et VIII; pour cela il faut considérer l'équation $Bx^2+by^2=az^2$, laquelle est impossible, parce que le premier membre est toujours de la forme $4n-1$ ou $4n-2$, tandis que le second membre est de la forme $4n$ ou $4n+1$. Mais l'équation dont il s'agit seroit résoluble, si l'on pouvoit satisfaire aux trois conditions

$$\left(\frac{Bb}{a}\right)=1,\quad \left(\frac{ab}{B}\right)=1,\quad \left(\frac{aB}{b}\right)=1.$$

Ee

Il faut donc que ces trois conditions soient incompatibles entre elles.

*Démonstration du cas VII.*

Soit $a = 1$, la première condition aura lieu d'elle-même, et les deux autres seront $\left(\frac{b}{B}\right) = 1$, $\left(\frac{B}{b}\right) = 1$. Celles-ci ne peuvent avoir lieu à-la-fois, donc

VII. Si l'on a $\left(\frac{B}{b}\right) = +1$, il s'ensuit $\left(\frac{b}{B}\right) = -1$.

*Démonstration du cas VIII.*

Soient toujours $B$ et $b$ les deux nombres qu'on veut comparer, et soit pris l'auxiliaire $a$, de manière qu'on ait $\left(\frac{a}{B}\right) = -1$, et $\left(\frac{a}{b}\right) = -1$, il s'ensuivra, par ce qui a été démontré $\left(\frac{B}{a}\right) = -1$, et $\left(\frac{b}{a}\right) = -1$. Donc des trois conditions précédentes, la première $\left(\frac{Bb}{a}\right) = 1$ a lieu d'elle-même, et les deux autres deviennent $\left(\frac{b}{B}\right) = -1$, $\left(\frac{B}{b}\right) = -1$. Celles-ci ne pourront avoir lieu simultanément. Donc

VIII. Si l'on a $\left(\frac{B}{b}\right) = -1$, il s'ensuit $\left(\frac{b}{B}\right) = +1$.

C'est le huitième et dernier cas de la proposition générale.

(169) En examinant les différentes parties de cette démonstration, on aura remarqué sans doute que les cas IV, V et VII sont démontrés directement et sans le secours d'aucune supposition. Quant aux autres cas, la démonstration est fondée sur l'existence d'un auxiliaire qui satisfait à deux conditions : ainsi les cas III et VI sont démontrés à l'égard de deux nombres quelconques $a$ et $b$, le premier de la forme $4n+1$, le second de la forme $4n-1$, en supposant qu'on peut trouver un nombre auxiliaire $A$ tel que

$\left(\frac{A}{a}\right)=-1$, et $\left(\frac{A}{b}\right)=-1$. Or il est facile de s'assurer qu'il y aura toujours une infinité de nombres premiers qui satisferont à ces conditions. En effet, en regardant $A$ comme inconnu, l'équation $\frac{A^{\frac{a-1}{2}}-1}{a}=e$ aura un nombre $\frac{a-1}{2}$ de solutions comprises entre o et $a$, ces solutions pouvant être paires ou impaires. Si on conserve les solutions impaires, et qu'on ajoute $a$ aux solutions paires, on aura le même nombre $\frac{a-1}{2}$ de solutions impaires comprises entre o et $2a$. Enfin si l'on ne conserve parmi ces solutions que celles de la forme $4n+1$, et si aux solutions restantes on ajoute $2a$, la tôtalité fera encore $\frac{a-1}{2}$ solutions de la forme $4n+1$, comprises entre o et $4a$. Soient ces solutions $\alpha$, $\alpha'$, $\alpha''$, $\alpha'''$, &c., et toutes les valeurs de $A$ qui satisfont à l'équation $\frac{A^{\frac{a-1}{2}}-1}{a}=e$, ou en d'autres termes à l'équation $\left(\frac{A}{a}\right)=1$, seront représentées par la formule $A=4az+[\alpha, \alpha', \alpha'', \alpha''', \text{\&c.}]$ qui signifie qu'à un multiple quelconque de $4a$ on peut ajouter celle qu'on voudra des $\frac{a-1}{2}$ quantités $\alpha$, $\alpha'$, $\alpha''$, &c. Maintenant de la suite 1, 5, 9, 13... $4a-3$ dont le nombre des termes est $a$, retranchez d'abord le terme $a$, ensuite tous les termes $\alpha$, $\alpha'$, $\alpha''$, $\alpha'''$, &c., il restera encore $\frac{a-1}{2}$ termes que je représente par (a), (a)', (a)'', (a)''', &c. et si l'on fait $A=4az+[(a), (a)', (a)'', (a)''', \text{\&c.}]$ ces nouvelles valeurs qui ne satisfont pas à l'équation $\left(\frac{A}{a}\right)=1$, satisferont nécessairement à l'équation $\left(\frac{A}{a}\right)=-1$.

Par un procédé semblable, on trouvera la formule $A=4bu+[(b), (b)', (b)'', (b)''', \text{\&c.}]$ dont toutes les valeurs parti-

culières satisfont à l'équation $\left(\frac{A}{b}\right)=-1$, et où les différens termes (b), (b)', (b)'', &c. sont toujours de la forme $4n+1$.

Maintenant chaque forme $4az+a$ peut être identifiée à chacune des formes $4bu+b$, et il en résulte une forme commune $A=4abx+c$; de sorte que les valeurs de $A$ qui satisfont à-la-fois aux deux conditions $\left(\frac{A}{a}\right)=-1$, $\left(\frac{A}{b}\right)=-1$ seront données par une formule $A=4abx+[c, c', c'', \&c.]$ dans laquelle les termes $c$, $c'$, $c''$, &c., tous de la forme $4n+1$ et tous moindres que $4ab$, seront au nombre de $\frac{a-1}{2}\cdot\frac{b-1}{2}$. Il ne s'agira donc plus que de prendre pour $A$ l'un des nombres premiers que cette formule générale doit contenir; nous ne mettons pas en doute qu'elle en contient, car on trouveroit aisément, par ce qui a été dit dans l'introduction, que ceux qui y sont contenus, constituent la huitième partie de tous les nombres premiers possibles.

(170) Le même raisonnement par lequel nous venons d'appuyer la démonstration des cas III et VI, s'applique presque littéralement au cas VIII; mais l'auxiliaire doit être déterminée un peu différemment dans les cas I et II. C'est pourquoi il ne sera pas inutile de ramener la démonstration de ces cas à quelque chose de plus simple.

Considérons, pour cet effet, l'équation impossible $x^2+Ay^2=abz^2$; cette équation seroit résoluble, si on pouvoit satisfaire aux trois conditions $\left(\frac{ab}{A}\right)=1$, $\left(\frac{A}{a}\right)=1$, $\left(\frac{A}{b}\right)=-1$. Supposons donc que $A$ et $a$ sont deux nombres donnés (toujours de la forme $4n+1$), et qu'on prenne l'auxiliaire $b$ de manière que $\left(\frac{A}{b}\right)=-1$, il en résultera $\left(\frac{b}{A}\right)=-1$; par ce moyen, la troisième condition sera satisfaite, et les deux autres deviendront $\left(\frac{a}{A}\right)=-1$, $\left(\frac{A}{a}\right)=1$. Ces deux dernières ne peuvent avoir lieu à-la-fois; donc

I. Si l'on a $\left(\frac{A}{a}\right) = 1$, il s'ensuit $\left(\frac{a}{A}\right) = 1$

II. Si l'on a $\left(\frac{a}{A}\right) = -1$, il s'ensuit $\left(\frac{A}{a}\right) = -1$.

Ainsi la démonstration des cas I et II ne suppose plus autre chose, sinon qu'on a $\left(\frac{A}{b}\right) = -1$, ou que le nombre auxiliaire $b$ divise la formule $x^2 + A$.

(171) C'est ici le lieu de placer quelques théorêmes assez importans, dont plusieurs ne peuvent se démontrer qu'à l'aide de la loi de réciprocité qu'on vient d'établir.

*Tout nombre premier* $4n+1$ *qui divise la formule* $t^2+au^2$, *est en même temps diviseur de la formule* $t^2-au^2$, *et réciproquement.*

Car soit $c$ ce nombre premier, la condition pour que $c$ divise $t^2+au^2$ est $\left(\frac{-a}{c}\right) = +1$, et la condition pour qu'il divise $t^2-au^2$ est $\left(\frac{a}{c}\right) = +1$ : or ces deux conditions reviennent à la même, parce que $\frac{c-1}{2}$ est pair. Donc si l'une a lieu, l'autre a lieu nécessairement.

On peut aussi démontrer la même proposition, en résolvant l'équation $\frac{x^2-a}{c} = e$ d'après l'équation donnée $\frac{\theta^2+a}{c} = e$; pour cela, il faut satisfaire à l'équation $\frac{x^2+\theta^2}{c} = e$. Or puisque $c$ est de la forme $4n+1$, on peut supposer d'abord $c = f^2+g^2$, ensuite on aura la valeur de $x$, au moyen de l'équation $fx - cy = g\theta$.

(172) *Tout nombre premier* $4n-1$ *qui divise* $t^2+au^2$, *ne peut être diviseur de* $t^2-au^2$, *et réciproquement.*

Car soit ce nombre premier $= c$, la condition pour que $c$ divise $t^2+au^2$, est $\left(\frac{-a}{c}\right) = 1$, ou $\left(\frac{a}{c}\right) = -1$; et la condition pour qu'il

divise $t^2 - au^2$ est $\left(\frac{a}{c}\right) = 1$ ; or ces deux conditions s'excluent mutuellement.

*Corollaire.* Tout nombre premier $4n-1$ divise nécessairement l'une des deux formules $t^2+au^2$, $t^2-au^2$ ; car on a toujours, ou $\left(\frac{a}{c}\right)=+1$, ou $\left(\frac{a}{c}\right)=-1$. On fait abstraction dans ce théorême, ainsi que dans le précédent, du cas où $c$ seroit diviseur de $a$ ; alors en effet on ne mettroit plus en question si $c$ divise $t^2+au^2$ ou $t^2-au^2$.

(173) *Si le nombre premier* c *divise les deux formules* $t^2 - au^2$, $t^2 - bu^2$, *il divisera également la formule* $t^2 - abu^2$.

Car ayant par hypothèse $\left(\frac{a}{c}\right) = 1$, $\left(\frac{b}{c}\right) = 1$, il s'ensuit que $\left(\frac{ab}{c}\right) = 1$, et qu'ainsi $c$ est diviseur de $t^2 - abu^2$.

Le même résultat auroit lieu pour un plus grand nombre de facteurs.

(174) *Si le nombre premier* c *ne divise ni la formule* $t^2 - au^2$, *ni la formule* $t^2 - bu^2$, *il divisera nécessairement la formule* $t^2 - abu^2$.

Car ayant par hypothèse $\left(\frac{a}{c}\right) = -1$, $\left(\frac{b}{c}\right) = -1$, il s'ensuit encore $\left(\frac{ab}{c}\right) = +1$ ; donc $c$ est diviseur de $t^2 - abu^2$.

(175) *Soient* a *et* A *des nombres premiers, tous deux de la forme* $4n+1$, *je dis que si* a *divise la formule* $t^2 + Au^2$, *réciproquement* A *divisera la formule* $t^2 + au^2$ ; *et si* a *ne divise point la formule* $t^2 + Au^2$, *réciproquement* A *ne divisera pas la formule* $t^2 + au^2$.

Car dans le premier cas on a $\left(\frac{-A}{a}\right) = 1$, c'est-à-dire $\left(\frac{A}{a}\right) = 1$ ; donc réciproquement $\left(\frac{a}{A}\right) = 1$ ; donc $A$ est diviseur de $t^2 + au^2$.

Dans le second cas, on auroit $\left(\frac{A}{a}\right) = -1$ ; d'où résulte éga-

lement $\left(\frac{a}{A}\right)=-1$; donc $A$ n'est point diviseur de $t^2+au^2$.

(176) *Soit* a *un nombre premier* $4n+1$, *et soient* A *et* B *deux nombres premiers quelconques tous deux diviseurs, ou tous deux non diviseurs de la formule* $t^2-au^2$, *je dis que* a *sera diviseur de la formule* $t^2-ABu^2$.

Car 1°. si $A$ et $B$ sont diviseurs de la formule $t^2-au^2$, on aura $\left(\frac{a}{A}\right)=1$, $\left(\frac{a}{B}\right)=1$; donc réciproquement $\left(\frac{A}{a}\right)=1$, $\left(\frac{B}{a}\right)=1$; donc $\left(\frac{AB}{a}\right)=1$, donc $a$ est diviseur de $t^2-ABu^2$.

2°. Si $A$ et $B$ sont non-diviseurs de la formule $t^2-au^2$, on aura $\left(\frac{a}{A}\right)=-1$, $\left(\frac{a}{B}\right)=-1$; d'où résulte $\left(\frac{A}{a}\right)=-1$, $\left(\frac{B}{a}\right)=-1$; donc on a encore $\left(\frac{AB}{a}\right)=+1$; donc $a$ est diviseur de $t^2-ABu^2$.

(177) *Soit* a *un nombre premier* $4n+1$, *et* b *un nombre premier* $4n-1$ *qui ne soit pas diviseur de* $t^2+au^2$, *je dis que* a *sera au contraire diviseur de* $t^2+bu^2$.

Car ayant par hypothèse $\left(\frac{-a}{b}\right)=-1$, ou $\left(\frac{a}{b}\right)=+1$, il s'ensuit $\left(\frac{b}{a}\right)=1$; donc $a$ est diviseur de $t^2+bu^2$.

En général, si on a plusienrs nombres premiers $b$, $b'$, $b''$ tous de la forme $4n-1$, et non-diviseurs de $x^2+a$, $a$ sera diviseur de la formule $t^2+bb'b''u^2$.

(178) *Tout nombre premier* c *de la forme* $8n+1$ *ou* $8n+7$, *divise à-la-fois les deux formules* $t^2+au^2$, $t^2+2au^2$, *ou ne divisera ni l'une ni l'autre.*

Car la valeur de $\left(\frac{-a}{c}\right)$ est la même que celle de $\left(\frac{-2a}{c}\right)$, puisque le nombre $c$ étant de l'une des deux formes mentionnées, on a toujours $\left(\frac{2}{c}\right)=1$ (n°. 148).

(179) *Tout nombre premier* c *de la forme* $8n+3$ *ou* $8n+5$, *divise toujours l'une des deux formules* $t^2+au^2$, $t^2+2au^2$, *mais n'en peut diviser qu'une.*

Car dans les formes mentionnées on a $\left(\frac{2}{c}\right)=-1$; donc les deux quantités $\left(\frac{-a}{c}\right)$ et $\left(\frac{-2a}{c}\right)$ sont de signes contraires. Donc il faut que l'une de ces quantités soit $+1$ et l'autre $-1$; d'où il suit que $c$ divise l'une des deux formules dont il s'agit, et ne divise pas l'autre.

*Remarquez* que dans ce théorême, ainsi que dans le précédent, $a$ est un nombre quelconque positif ou négatif.

(180) Nous ne nous arrêterons pas à multiplier davantage ces sortes de théorêmes, mais nous croyons que les Géomètres verront avec plaisir l'application de notre loi de réciprocité à la démonstration de deux conclusions générales auxquelles Euler est parvenu, par voie d'induction, dans ses *Opuscula Analytica*, tom. I, et qui sont la base d'une théorie importante. La première est conçue à-peu-près en ces termes : (Voyez l'ouvrage cité, pag. 276.)

« *Si tous les quarrés successifs* 1, 4, 9, 16, &c. *sont divisés* » *par un même nombre premier* $4n+1$, *les restes des divisions* » *comprendront non-seulement tous les nombres contenus dans les* » *formules* $n-qq-q$ *et* $qq+q-n$, *mais encore tous les facteurs* » *premiers dont ces nombres sont composés* ».

D'abord il est facile de voir, que puisque $c=4n+1$, on satisfera à l'équation $\frac{xx+n-qq-q}{c}=e$, en prenant $2x=2q+1\pm c$. D'ailleurs $c$ étant de la forme $4n+1$, si l'équation $\frac{x^2+a}{c}=e$ est possible, l'équation $\frac{y^2-a}{c}$ l'est également; donc, en effet, tout nombre compris, soit dans la formule $n-qq-q$, soit dans la formule $qq+q-n$, ou ce nombre diminué d'un multiple de $c$, peut être regardé comme le reste d'un quarré divisé par $c$. Cette première partie du théorême ne souffre aucune difficulté, ainsi qu'Euler

qu'Euler lui-même l'a fait voir. Venons à la seconde qui exige l'emploi de la loi de réciprocité.

Soit $\alpha$ un nombre premier qui divise $n-qq-q$ ou $qq+q-n$, on pourra faire $qq+q-n=\pm\alpha A$; donc en multipliant par 4, puis mettant au lieu de $4n$ sa valeur $c-1$, on aura

$$(2q+1)^2-c=\pm 4\alpha A.$$

De-là, en omettant les multiples de $\alpha$, on tire $c=(2q+1)^2$; donc $c^{\frac{\alpha-1}{2}}$ ou suivant notre notation $\left(\frac{c}{\alpha}\right)=(2q+1)^{\alpha-1}=1$. Mais de ce que $\left(\frac{c}{\alpha}\right)=1$, il s'ensuit par la loi de réciprocité $\left(\frac{\alpha}{c}\right)=1$; donc $c$ est diviseur de la formule $x^2-\alpha$. Donc $\alpha$ doit se trouver parmi les restes des quarrés divisés par le nombre premier $c$, ce qui est la proposition d'Euler.

(181) La seconde conclusion générale (Voyez l'ouvrage cité, pag. 281) est celle-ci.

« *Si l'on divise les quarrés* 1, 4, 9, 16, &c. *par le nombre premier* $4n-1$, *les restes des divisions comprendront non-seulement tous les nombres représentés par la formule* $n+qq+q$, *mais encore tous les facteurs premiers dont ces nombres sont composés* ».

Pour satisfaire à la première partie, il faut trouver un nombre $x$ tel que $x^2-(n+qq+q)$ soit divisible par le nombre premier $c=4n-1$; or c'est ce que l'on obtiendra immédiatement, en prenant $2x=2q+1\pm c$. Donc le nombre $n+qq+q$, ou ce nombre diminué d'un multiple de $c$, est toujours le reste d'un quarré $x^2$ divisé par $c$.

Soit en second lieu $\alpha$ un nombre premier qui divise $n+qq+q$, si l'on fait $n+qq+q=\alpha A$, on en déduira comme ci-dessus, $(2q+1)^2+c=4\alpha A$. Donc en omettant les multiples de $\alpha$, on a $c=-(2q+1)^2$; donc $\left(\frac{-c}{\alpha}\right)=1$. Cela posé, il y a deux cas à distinguer.

1°. Si $\alpha$ est de la forme $4m+1$, l'équation $\left(\frac{-c}{\alpha}\right)=1$ est la

même que $\left(\frac{c}{\alpha}\right)=1$, et on en déduit par la loi de réciprocité $\left(\frac{\alpha}{c}\right)=1$ ; donc $c$ est diviseur de $x^2-\alpha$.

2°. Si $\alpha$ est de la forme $4m-1$, l'équation $\left(\frac{-c}{\alpha}\right)=1$, donne $\left(\frac{c}{\alpha}\right)=-1$, et on en déduit par la loi de réciprocité $\left(\frac{\alpha}{c}\right)=1$ ; donc $c$ est encore diviseur de $x^2-\alpha$.

Donc, dans tous les cas, le nombre premier $\alpha$, ou ce nombre diminué d'un multiple de $c$, est le reste d'un quarré divisé par $c$, et par conséquent doit se trouver parmi les restes que donnent les différens termes de la suite 1, 4, 9, 16, &c. divisés par $c$.

---

## §. VII. *Usage du théorême précédent pour connoître si un nombre premier* c *divise la formule* $x^2+a$. *Des cas où l'on peut déterminer* a priori *le nombre* x.

(182) Lorsque $c$ est un nombre un peu grand, et qu'on a besoin de savoir si $c$ est diviseur de $x^2+a$, il peut être fort long d'élever $a$ à la puissance $\frac{c-1}{2}$, même en abrégeant l'opération autant qu'il est possible, et en ayant soin d'omettre les multiples de $c$ à mesure qu'ils se présentent. Voici un procédé que fournit le théorême précédent, et qui conduit très-promptement à la valeur cherchée de $\left(\frac{a}{c}\right)$.

1°. Si $a$ est plus grand que $c$, on mettra, au lieu de $a$, le reste de la division de $a$ par $c$; ainsi on pourra toujours supposer que $a$ est plus petit que $c$. En effet, on voit bien que $(mc+a)^{\frac{c-1}{2}}$ divisé par $c$, laissera le même reste que $a^{\frac{c-1}{2}}$.

2°. Si le nombre $a$ (ainsi réduit) est un nombre premier, l'expression $\left(\frac{a}{c}\right)$ se changera suivant le théorême, soit en $\left(\frac{c}{a}\right)$ soit en $-\left(\frac{c}{a}\right)$, ce dernier cas n'ayant lieu que lorsque $a$ et $c$ sont tous deux de la forme $4n-1$. Mais puisque $c$ est $>a$, on peut, au lieu de $c$, prendre le reste de la division de $c$ par $a$; soit ce reste $c'$, on aura donc $\left(\frac{c}{a}\right)=\left(\frac{c'}{a}\right)$, et ainsi la question concernant la valeur de $\left(\frac{a}{c}\right)$ est réduite à une question semblable sur l'expression $\left(\frac{c'}{a}\right)$ qui est composée de plus petits nombres; la résolution se fera donc ultérieurement, tant par ce qui a été déjà dit que par ce que nous allons ajouter.

3°. Si $a$ n'est pas premier, décomposez $a$ en ses facteurs premiers $\alpha$, $\beta$, $\gamma$.... parmi lesquels 2 peut être compris, vous aurez $\left(\frac{a}{c}\right)=$ au produit des expressions $\left(\frac{\alpha}{c}\right)$ $\left(\frac{\beta}{c}\right)$ $\left(\frac{\gamma}{c}\right)$ &c. Omettez parmi les facteurs $\alpha$, $\beta$, $\gamma$, ceux qui sont quarrés, car en général $\left(\frac{\alpha^2}{c}\right)$ représente le reste de $\alpha^{c-1}$ divisé par $c$, lequel reste est toujours 1; observez de plus 1°. qu'on a $\left(\frac{2}{c}\right)=+1$, si $c$ est de la forme $8n\pm1$, et qu'on a $\left(\frac{2}{c}\right)=-1$, si $c$ est de la forme $8n\pm3$. 2°. Qu'on a $\left(\frac{-m}{c}\right)=\left(\frac{m}{c}\right)$, si $c$ est de la forme $4n+1$, et qu'on a $\left(\frac{-m}{c}\right)=-\left(\frac{m}{c}\right)$, si $c$ est de la forme $4n-1$.

Au moyen de ces préceptes et des renversemens donnés par le théorême du §. précédent, on trouvera bientôt la valeur de l'expression proposée $\left(\frac{a}{c}\right)$. Et l'opération, assez semblable à celle par laquelle on cherche le plus grand commun diviseur de deux nombres, sera à-peu-près aussi expéditive.

EXEMPLE I.

(183) Pour avoir la valeur de l'expression $\left(\frac{601}{1013}\right)$ j'observe que ces deux nombres sont premiers, et j'aurai, en vertu du théorême $\left(\frac{601}{1013}\right)=\left(\frac{1013}{601}\right)$; la division de 1013 par 601 donne 412 de reste, et 412 étant le produit de 4 par 103, on peut omettre le facteur quarré 4, ce qui donnera $\left(\frac{601}{1013}\right)=\left(\frac{103}{601}\right)$. Mais 103 étant encore un nombre premier, on a par le théorême, $\left(\frac{103}{601}\right)$ $=\left(\frac{601}{103}\right)=$ (en divisant 601 par 103 et ne conservant que le reste) $\left(\frac{86}{103}\right)=\left(\frac{2}{103}\right)\cdot\left(\frac{43}{103}\right)=$ (parce que $\left(\frac{2}{103}\right)=1$)

$\left(\frac{43}{103}\right) = -\left(\frac{103}{43}\right) = -\left(\frac{17}{43}\right) = -\left(\frac{43}{17}\right) = -\left(\frac{9}{17}\right) = -1$. Donc $\left(\frac{601}{1013}\right) = -1$. Donc 1013 n'est pas diviseur de $x^2+601$.

Pour faire la même vérification par la voie ordinaire, il auroit fallu élever 601 à la puissance 506, en rejetant les multiples de 1013 à mesure qu'ils se présentent. Or 506 exprimé en chiffres de l'arithmétique binaire (1) est 111 111 010, c'est-à-dire en d'autres termes que 506 est la somme des puissances de 2, dont les exposans sont 8, 7, 6, 5, 4, 3, 1. Pour former les puissances de 601 qui ont ces puissances de 2 pour exposans, il faut faire huit multiplications ou élévations au quarré; ensuite, pour multiplier entr'elles les diverses puissances de 601 dont les exposans sont $2^8$, $2^7$, $2^6$, $2^5$, $2^4$, $2^3$, $2^1$, il faut encore six multiplications; de sorte qu'il faut en tout 14 multiplications, et autant de divisions par 1013 pour arriver au résultat final. Voici au reste le détail de l'opération, afin qu'on puisse mieux comparer les deux méthodes; on n'a mis que les restes des divisions par 1013.

| | |
|---|---|
| $(601)^2 = 573$ | $(601)^{384} = 89 \times 525 = 127$ |
| $(601)^4 = (573)^2 = 117$ | $(601)^{448} = 127 \times -437 = +216$ |
| $(601)^8 = (117)^2 = 520$ | $(601)^{480} = +216 \times -24 = -119$ |
| $(601)^{16} = (520)^2 = -71$ | $(601)^{496} = -119 \times -71 = 345$ |
| $(601)^{32} = (71)^2 = -24$ | $(601)^{504} = 345 \times 520 = 99$ |
| $(601)^{64} = (24)^2 = -437$ | $(601)^{506} = 99 \times 573 = -1$. |
| $(601)^{128} = (437)^2 = 525$ | Donc en effet $\left(\frac{601}{1013}\right) = -1$. |
| $(601)^{256} = (525)^2 = 89$ | |

(1) Voici un moyen très-court d'exprimer un nombre un peu grand en caractères binaires. Soit par exemple le nombre 11183445 dont il sera question dans l'exemple III, je divise ce nombre par 64, j'ai le reste 21 et le quotient 174741; celui-ci, divisé par 64, donne le reste 21 et le quotient 2730; enfin 2730 divisé par 64, donne le reste 42 et le quotient 42: mais 21 s'exprime en chiffres binaires par 10101 et 42 par 101010. Donc le nombre proposé s'exprimera par 101010 101010 010101 010101.

EXEMPLE II.

(184) On demande la valeur de $\left(\frac{402}{929}\right)$?

Pour cela je décompose 402 en ses trois facteurs 2.3.67, et j'ai $\left(\frac{402}{929}\right)=\left(\frac{2}{929}\right)\cdot\left(\frac{3}{929}\right)\cdot\left(\frac{67}{929}\right)$. Or on a

$$\left(\frac{2}{929}\right)=1$$

$$\left(\frac{3}{929}\right)=\left(\frac{929}{3}\right)=\left(\frac{2}{3}\right)=-1$$

$$\left(\frac{67}{929}\right)=\left(\frac{929}{67}\right)=\left(\frac{-9}{67}\right)=-\left(\frac{1}{67}\right)=-1;$$

et le produit de ces trois résultats est $+1$, donc $\left(\frac{402}{929}\right)=+1$; donc 929 est diviseur de $t^2 \pm 402u^2$, ou de $x^2 \pm 402$.

EXEMPLE III.

(185) Prenons un nombre premier très-grand, tel que 22 366 891, et cherchons si ce nombre est diviseur de $x^2+1459$?

Il faut donc avoir la valeur de $\left(\frac{1459}{22\,366\,891}\right)$; et parce que 1459 est également un nombre premier $4n-1$, cette valeur $=-\left(\frac{22\,366\,891}{1459}\right)=-\left(\frac{421}{1459}\right)=-\left(\frac{1459}{421}\right)=-\left(\frac{196}{421}\right)=-1$, (parce que 196 est un quarré). Donc la valeur cherchée est $-1$. Donc 22 366 891 est diviseur de $x^2+1459$.

C'est ce qu'on n'auroit pu trouver par la voie ordinaire, qu'en faisant 34 multiplications et autant de divisions très-laborieuses, puisque le diviseur seroit 22 366 891.

(186) Après s'être assuré que le nombre premier $c$ est diviseur de $x^2+a$, il reste à déterminer la valeur de $x$ qui rend la division possible. C'est ce qu'on peut faire *a priori* dans quelques cas généraux que nous allons indiquer.

1°. Lorsque $c=4n-1$, la condition de possibilité donne

$(-a)^{2n-1}-1$ divisible par $c$ ; donc $a^{2n}+a$ est divisible par $c$ ; donc si on prend $x=a^n$ ou égal au reste de $a^n$ divisé par $c$, on sera sûr que $\frac{x^2+a}{c}$ est un entier. Ce premier cas très-général comprend déjà la moitié de tous les cas possibles. Il ne reste donc plus à examiner que le cas de $c=4n+1$, lequel comprend les deux formes $8n+1$, $8n+5$.

2°. Lorsque $c=8n+5$, la condition de possibilité exige que $a^{4n+2}-1$ soit divisible par $c$; mais cette quantité est le produit des deux facteurs $a^{2n+1}+1$, $a^{2n+1}-1$, il faut donc que l'un de ces facteurs soit divisible par $c$. Si le facteur $a^{2n+1}+1$ est divisible par $c$, faites $x=a^{n+1}$, et vous aurez $\frac{x^2+a}{c}=e$. Si c'est l'autre facteur qui est divisible par $c$, faites de même $\theta=a^{n+1}$, et vous aurez $\frac{\theta^2-a}{c}=e$; dans ce dernier cas, il ne reste plus qu'à satisfaire à l'équation $\frac{x^2+\theta^2}{c}=e$. Or puisque $c$ est de la forme $4m+1$, on peut supposer $c=f^2+g^2$; cherchant ensuite les indéterminées $p$ et $q$ d'après l'équation

$$\theta=fp+gq,$$

on en conclura $x=fq-gp$; car de-là résulte $x^2+\theta^2=(f^2+g^2)(p^2+q^2)$; donc $x^2+\theta^2$, et par suite $x^2+a$ est divisible par $c$.

3°. Le dernier cas à considérer, est celui de $c=8n+1$, mais alors on ne peut pas toujours satisfaire à l'équation $\frac{x^2+a}{c}=e$ d'une manière directe et sans tâtonnement. Soit $n=\alpha\zeta$, $\zeta$ étant un nombre impair et $\alpha$ une puissance de 2, la condition de possibilité exigeant que $a^{4\alpha\zeta}-1$ soit divisible par $c$, il pourra arriver que $a^{\zeta}\pm 1$ soit divisible par $c$, et alors à cause de $\zeta$ impair, on trouvera la valeur de $x$ de la même manière qu'on l'a trouvée lorsque $c=8n+5$.

Si $a^{\zeta}\pm 1$ n'est pas divisible par $c$, on ne trouve pas de solution *a priori* ; ainsi pour résoudre l'équation $\frac{x^2+a}{c}=e$, il faudra

calculer les différens termes de la suite $c-a$. $2c-a$, $3c-a$, $4c-a$, &c., jusqu'à ce qu'on en trouve un qui soit un quarré parfait et qui donnera la valeur de $x^2$; cette suite, au reste, contiendra nécessairement le quarré qu'on cherche, quarré qui doit être moindre que $\frac{1}{4}c^2$, ainsi le nombre de termes à calculer ne peut excéder $\frac{1}{4}c$.

Par exemple, si l'on a à résoudre l'équation $\frac{x^2+229}{641}=e$, dont la possibilité est déjà établie par la condition $\left(\frac{229}{641}\right)=1$, il faudra former les différens termes de la progression arithmétique dont le terme général est $641e-229$. Cette progression est 412, 1053, 1694, 2335, &c. mais il faut la continuer jusqu'au 94$^{\text{ème}}$ terme avant qu'on trouve le quarré 60025 dont la racine $245=x$. Il est vrai qu'on peut passer sur beaucoup de termes, lorsqu'on prévoit que le chiffre qui les termine n'est pas un de ceux qui conviennent aux quarrés (1). Mais le travail est encore assez long par cette voie, lorsque le nombre cherché $x$ n'est pas beaucoup plus petit que $\frac{1}{2}c$.

(187) Pour rendre cette détermination moins laborieuse, on pourra avoir recours aux propriétés des diviseurs qui seront démontrées ci-après. En vertu de ces propriétés, tout diviseur de la formule $t^2+au^2$ est lui-même de la forme $y^2+az^2$, ou au moins il devient de cette forme, en le multipliant par un nombre $p$

(1) Le quarré de $10m+n$ est $100m^2+20mn+n^2$, donc le chiffre qui termine le quarré de $10m+n$, est le même que celui qui termine le quarré de $n$. Mais les nombres 0, 1, 2, 3... 9 ont leurs quarrés terminés par l'un des chiffres 0, 1, 4, 5, 6, 9; donc aucun quarré ne peut être terminé par 2, 3, 7, 8. On peut ajouter à cette observation, 1°. que si le dernier chiffre d'un quarré est 0, il faut que les deux derniers soient deux zéros. 2°. Que si le dernier chiffre est 5, les deux derniers doivent être 25. 3°. Que si le dernier chiffre est impair, l'avant-dernier doit être pair. 4°. Que si le dernier chiffre est 4, l'avant-dernier doit être pair, afin que tout le nombre soit divisible par 4. 5°. Que si le dernier chiffre est 6, l'avant-dernier doit être impair par la même raison.

moindre

moindre que $2\sqrt{\frac{a}{3}}$. Supposons donc qu'on a trouvé $pc=f^2+ag^2$, on cherchera $x$ d'après l'équation,

$$f=gx+cy,$$

et la valeur de $x$ sera telle, que $x^2+a$ est divisible par $c$.

Ainsi, dans l'exemple précédent, on reconnoît bientôt que 641 n'est pas de la forme $f^2+229g^2$, mais il le devient, étant multiplié par 14, car on a $641\times 14=8974=57^2+229.5^2$; faisant donc $57=5x+641y$, on trouvera $x=-245$. Cette méthode peut faire éviter beaucoup de tâtonnement, et elle sera sur-tout utile lorsque le nombre $a$ est peu considérable; car les tables feront connoître, d'après la forme $4az+a$ du nombre $c$, quel est le multiplicateur $p$ qui peut rendre le produit $pc$ de la forme $f^2+ag^2$.

---

## §. VIII. *De la manière de déterminer* x *pour que* $x^2+a$ *soit divisible par un nombre composé quelconque* N.

(188) Soit $c$ un nombre premier, et $a$ un nombre quelconque non-divisible par $c$, si l'on demande la valeur de $x$ telle que $x^2+a$ soit divisible par $c^m$, cherchez d'abord par ce qui précède la valeur de $\theta$ qui rend $\theta^2+a$ divisible par $c$; faites ensuite $(\theta+\sqrt{-a})^m = p+q\sqrt{-a}$; vous aurez de même $(\theta-\sqrt{-a})^m = p-q\sqrt{-a}$, et le produit de ces deux équations donnera $(\theta^2+a)^m = p^2+aq^2$, donc $p^2+aq^2$ est divisible par $c^m$. Dans ce résultat, $q$ et $c$ sont premiers entr'eux; ainsi on pourra supposer $p=qx+c^m y$, et $x^2+a$ sera divisible par $c^m$, ce qui est la question proposée.

Nous venons de supposer que $q$ n'est point divisible par $c$; car s'il l'étoit, $p$ le seroit aussi en vertu de l'équation $(\theta^2+a)^m = p^2+aq^2$ dont le premier membre est divisible par $c^m$. Mais on a

$$p = \theta^m - \frac{m.m-1}{1.2}\theta^{m-2}a + \frac{m.m-1.m-2.m-3}{1.2.3.4}\theta^{m-4}a^2 - \&c.$$

Et puisque $\theta^2+a$ est divisible par $c$, on peut mettre $-\theta^2+Ac$ à la place de $a$, ce qui donnera $p$ de cette forme

$$p = \theta^m\left(1 + \frac{m.m-1}{1.2} + \frac{m.m-1.m-2.m-3}{1.2.3.4} + \&c.\right) + Bc,$$

ou $p = 2^{m-1}\theta^m + Bc$; mais $\theta$ n'est point divisible par $c$, donc $p$ ne peut l'être, ni par conséquent $q$.

Si le nombre $a$ est divisible par $c$, la quantité $x^2+a$ sera divisible par $c$, en prenant $x=0$ ou un multiple de $c$; mais il sera souvent impossible que $x^2+a$ soit divisible par $c^2$ ou par une puissance plus élevée de $c$; par exemple, si $a$ est divisible par $c$ et non par $c^2$, il est évident que jamais $x^2+a$ ne peut être divisible par $c^2$.

(189) Il est facile maintenant de trouver, lorsque cela est possible, la valeur de $x$, telle que $x^2+a$ soit divisible par un nombre composé quelconque $N$.

1°. Si $N$ et $a$ sont premiers entr'eux, on décomposera $N$ en ses facteurs premiers impairs $\alpha^\lambda \mathcal{C}^\mu \gamma^\nu$ &c., et on cherchera, par la méthode qui précède les nombres $A$, $B$, $C$, &c. tels que les quantités

$$\frac{A^2+a}{\alpha^\lambda}, \quad \frac{B^2+a}{\mathcal{C}^\mu}, \quad \frac{C^2+a}{\gamma^\nu}, \quad \&c.$$

soient des entiers, il faudra ensuite satisfaire aux équations indéterminées

$$x = A+\alpha^\lambda y = \pm B+\mathcal{C}^\mu z = \pm C+\gamma^\nu u = \&c.$$

Et il est facile de voir que $x^2+a$ étant divisible par chacun des facteurs $\alpha^\lambda$, $\mathcal{C}^\mu$, $\gamma^\nu$, &c., sera divisible par leur produit $\alpha^\lambda \mathcal{C}^\mu \gamma^\nu$ &c.

Si outre les facteurs impairs $\alpha^\lambda$, $\mathcal{C}^\mu$, &c., $N$ contient le facteur $2^k$, il faudra combiner les valeurs précédentes avec celle qui résulte de l'équation $\frac{x^2+a}{2^k}=e$ : or cette équation, si elle est possible, sera toujours facile à résoudre.

Soit, par exemple, l'équation $\frac{x^2+15}{2^{10}}=e$, on voit d'abord qu'en faisant $x=1$, $x^2+15$ est divisible par $2^4$. On fera, en conséquence, $x=1+2^3y$, ce qui donnera $\frac{1+y+4y^2}{2^6}=e$; celle-ci fait voir que $1+y$ doit être divisible par 4. Soit donc $y=4z-1$, et l'équation à résoudre deviendra $\frac{1-7z}{16}=e$; d'où l'on tire $z=7$, $y=27$ et $x=217$.

Nous observerons que lorsque $k$ est plus grand que 2, il y a toujours deux manières de satisfaire à l'équation $\frac{x^2+a}{2^k}=e$, car si une solution, moindre que $\frac{1}{2}2^k$, est désignée par $\theta$, l'autre sera $2^{k-1}-\theta$. De sorte que dans l'exemple précédent, la seconde solution seroit $2^9-217$ ou 295.

2°. Si les nombres $N$ et $a$ ne sont pas premiers entr'eux, soit $\psi^2\omega$ leur plus grand commun diviseur, $\psi^2$ étant le plus grand quarré contenu dans $\psi^2\omega$, et par conséquent $\omega$ ne pouvant plus avoir que des facteurs simples; alors il faudra faire $N=\psi^2\omega N'$, $a=\psi^2\omega a'$,

$x = \psi\omega x'$, et l'équation à résoudre $\frac{x^2 + a}{N} = e$, deviendra $\frac{\omega x'^2 + a'}{N'} = e$. Dans celle-ci $\omega$ et $N'$ doivent être premiers entr'eux, car s'ils avoient un commun diviseur $\pi$, il faudroit que $a'$ fût aussi divisible par $\pi$ (sans quoi l'équation à résoudre seroit impossible); donc $\omega^2\psi$ ne seroit pas le plus grand commun diviseur de $a$ et $N$, contre la supposition.

Puisque $\omega$ et $N'$ sont premiers entr'eux, on pourra trouver deux entiers $f$ et $g$ tels qu'on ait $f\omega - gN' = 1$; multipliant donc par $f$ l'équation $\frac{\omega x'^2 + a'}{N} = e$, et mettant $gN' + 1$ à la place de $f\omega$, cette équation deviendra $\frac{x'^2 + fa'}{N'} = e$; et ainsi la question est ramenée au cas précédent où $N$ et $\omega$ sont premiers entr'eux.

Il faut maintenant examiner combien dans ces différens cas l'équation $\frac{x^2 + a}{N} = e$ pourra avoir de solutions ou valeurs de $x$ moindres que $\frac{1}{2}N$.

(190) *Si* N *est impair et premier à* a, *le nombre de solutions de l'équation* $\frac{x^2 + a}{N} = e$, *sera* $2^{i-1}$, i *étant le nombre des facteurs premiers différens qui divisent* N.

Soit d'abord $N = \alpha^\lambda$; $\alpha$ étant un nombre premier, je dis qu'il n'y aura qu'une manière de satisfaire à l'équation $\frac{x^2 + a}{N} = e$. Car s'il y avoit deux solutions désignées par $x$ et $x'$, il faudroit que $x^2 - x'^2$ fût divisible par $\alpha^\lambda$; et comme aucun des facteurs $x + x'$, $x - x'$ n'est divisible par $\alpha^\lambda$, puisque $x$ et $x'$ sont supposés inégaux et plus petits que $\frac{1}{2}\alpha^\lambda$, il faudra que ces facteurs $x + x'$, $x - x'$ soient tous deux divisibles par $\alpha$, donc leur somme $2x$ seroit également divisible par $\alpha$; mais si $x$ étoit divisible par $\alpha$, il faudroit que $a$ le fût aussi, d'après l'équation $\frac{x^2 + a}{\alpha^\lambda} = e$. Donc puisque $a$ et $N$ sont premiers entr'eux, l'équation $\frac{x^2 + a}{\alpha^\lambda} = e$ ne pourra avoir qu'une solution moindre que $\frac{1}{2}\alpha^\lambda$.

Soit en second lieu $N=\alpha^{\lambda}\,6^{\mu}$, et soient $A$ et $B$ les valeurs de $x$ qui satisfont aux équations $\frac{x^2+a}{\alpha^{\lambda}}=e$, $\frac{x^2+a}{6^{\mu}}=e$; si on combine ensemble (n°. 14) les deux valeurs $x=A+\alpha^{\lambda}y$, $y=\pm B+6^{\mu}z$, il est clair qu'on aura, à cause du signe $\pm$, deux valeurs de $x$ de la forme $x=K+\alpha^{\lambda}\,6^{\mu}x'=K+Nx'$, chacune desquelles peut être rendue moindre que $\frac{1}{2}N$ en prenant pour $x'$ la valeur convenable. Donc dans le cas des deux facteurs inégaux $\alpha$, $6$, l'équation proposée aura deux solutions.

S'il y a un troisième facteur $\gamma^{\nu}$, il faudra combiner la valeur trouvée $x=K+\alpha^{\lambda}\,6^{\mu}x'$, avec une troisième formule $x=\pm C+\gamma^{\nu}z$, et il est évident que l'on aura quatre solutions de la forme $K'+\alpha^{\lambda}\,6^{\mu}\gamma^{\nu}x''$, ou $K'+Nx''$, lesquelles pourront être rendues moindres que $\frac{1}{2}N$.

En général, chaque nouveau facteur double le nombre des solutions obtenues par les facteurs précédens. Donc on aura en tout $2^{i-1}$ solutions, $i$ étant le nombre des facteurs $\alpha^{\lambda}, 6^{\mu}, \gamma^{\nu}$, &c. dont $N$ est composé.

*Remarque.* Toutes choses restant les mêmes, l'équation $\frac{x^2+a}{2N}=e$ aura également $2^{i-1}$ solutions. Car si $\theta$ est une valeur de $x$ qui rend $x^2+a$ divisible par $N$, cette même valeur $\theta$, ou au moins $N-\theta$, rendra $x^2+a$ divisible par $2N$.

(191) *Soit* N *impair ou double d'un impair, si les deux nombres* N *et* a *ont un commun diviseur* $\omega$, *lequel ne soit divisible par aucun quarré, je dis que l'équation* $\frac{x^2+a}{N}=e$ *aura toujours* $2^{i-1}$ *solutions,* i *étant le nombre de facteurs premiers impairs et inégaux qui divisent* N *sans diviser* a.

En effet, soit $N=\omega N'$, $a=\omega x'$, l'équation proposée deviendra $\frac{\omega x'^2+a'}{N'}=e$, et parce que $\omega$ et $N'$ n'ont pas de commun diviseur, on peut faire $f\omega-gN'=1$, ce qui donnera l'équation réduite

$\frac{x'^2+fa'}{N'}=e$. Or celle-ci, où $N'$ et $fa'$ sont premiers entr'eux, admet autant de solutions qu'il y a d'unités dans $2^{i-1}$, $i$ étant le nombre de facteurs premiers impairs et inégaux qui divisent $N'$; et si l'on fait en général $x'=\theta+N'x''$, on aura $x=\omega\theta+\omega N'x''=\omega\theta+Nx''$. Donc il y aura autant de valeurs de $x$ moindres que $\frac{1}{2}N$ qu'il y a de valeurs de $x'$ moindres que $\frac{1}{2}N'$; donc le nombre de ces valeurs est égal à $2^{i-1}$.

(192) *Si le nombre* N, *impair ou double d'un impair, a un commun diviseur quelconque avec* a, *et que ce diviseur soit représenté par* $\omega\psi^2$, *en sorte qu'on ait* $\mathrm{N}=\psi^2\omega\mathrm{N}'$, $\omega$ *n'étant divisible par aucun quarré, je dis que l'équation* $\frac{\mathrm{x}^2+\mathrm{a}}{\mathrm{N}}=e$ *aura autant de solutions qu'il y a d'unités dans* $\psi.2^{i-1}$, i *étant le nombre de facteurs premiers impairs et inégaux qui divisent* N'.

Car dans ce cas, on a $a=\psi^2\omega a'$, $x=\psi\omega x'$, et l'équation à résoudre devient $\frac{\omega x'^2+a'}{N'}=e$, laquelle, comme on a vu dans le n°. précédent, donne $2^{i-1}$ valeurs de $x'$ moindres que $\frac{1}{2}N'$. Soit en général $x'=\theta+N'x''$, on aura donc $x=\psi\omega\theta+\psi\omega N'x''$; or comme il suffit que les valeurs de $x$ soient moindres ou non plus grandes que $\frac{1}{2}N=\frac{1}{2}\psi^2\omega N'$, il est clair qu'on peut donner à $x''$ les valeurs successives $0$, $\pm1$, $\pm2$, &c. jusqu'à $\pm\frac{1}{2}(\psi-1)$. Le nombre de ces valeurs est évidemment $\psi$; donc chaque valeur de $x'$ moindre que $\frac{1}{2}N'$, donnera $\psi$ valeurs de $x$ moindres que $\frac{1}{2}N$; donc le nombre de toutes les valeurs de $x$ sera $\psi.2^{i-1}$.

*Remarque.* Cette formule est vraie, même lorsque $i=0$, c'est-à-dire lorsque le nombre $N$ ou au moins sa moitié est diviseur de $a$; alors elle se réduit à $\frac{1}{2}\psi$, mais il faudra compter comme entier la fraction contenue dans $\frac{1}{2}\psi$, de sorte que si $\psi=2h+1$, on prendra $h+1$ pour $\frac{1}{2}\psi$.

## §. IX. *Résolution des équations symboliques* $\left(\frac{x}{c}\right)=1$, $\left(\frac{x}{c}\right)=-1$, c *étant un nombre premier.*

(193) Soit $c$ un nombre premier quelconque, et soit proposé de trouver toutes les valeurs de $x$ qui satisfont à l'équation $\left(\frac{x}{c}\right)=1$, ou $\frac{x^{\frac{c-1}{2}}-1}{c}=e$. Il est aisé de voir qu'on peut faire $x=y^2$, $y$ étant un nombre quelconque non divisible par $c$; les différentes valeurs de $x$ seront donc 1, 4, 9, 16.... jusqu'à $\left(\frac{c-1}{2}\right)^2$ inclusivement, ces valeurs peuvent être abaissées toutes au-dessous de $c$, en retranchant les multiples de $c$ qui y sont compris, et leur nombre est, comme on voit, $\frac{c-1}{2}$; il ne peut être plus grand, parce que l'exposant de $x$ n'est que $\frac{c-1}{2}$; il n'est pas moindre non plus, car si deux quarrés $m^2$, $n^2$, chacun moindres que $\left(\frac{c+1}{2}\right)^2$, laissoient le même reste ou la même valeur de $x$, il faudroit que $m^2-n^2$ fût divisible par $c$, ce qui ne peut être, parce que $m-n$ et $m+n$ sont tous les deux moindres que $c$. Nous connoissons donc les $\frac{c-1}{2}$ solutions de l'équation $\left(\frac{x}{c}\right)=1$, ces solutions étant comprises entre $o$ et $c$; mais comme il s'agit seulement des solutions en nombres impairs, parmi les valeurs de $x$ on conservera les nombres impairs, et on ajoutera $c$ aux nombres pairs, ce qui fera encore $\frac{c-1}{2}$ solutions impaires comprises depuis 1 jusqu'à $2c-1$.

Pour parvenir immédiatement à ces solutions, on formera, par

le moyen des différences, la suite des quarrés impairs, comme on le voit ici :

Differ. 8 16 24 32 40 48 56
Quar. 1, 9, 25, 49, 81, 121, 169, 225, &c.

On retranchera, tant dans les différences que dans les quarrés, les multiples de $2c$ à mesure qu'ils se présenteront, et la suite des quarrés, ou plutôt de leurs résidus, continuée jusqu'à $\frac{c-1}{2}$ termes, contiendra toutes les solutions de l'équation $\left(\frac{x}{c}\right)=1$, impaires, positives et moindres que $2c$. Ensuite ces solutions pourront être augmentées d'un multiple quelconque de $2c$, ce qui donnera $x=2cz+b$, $b$ ayant $\frac{c-1}{2}$ valeurs différentes.

Connoissant ainsi toutes les solutions de l'équation $\left(\frac{x}{c}\right)=1$, on aura par voie d'exclusion toutes celles de l'équatiou $\left(\frac{x}{c}\right)=-1$. Car les nombres impairs, moindres que $2c$, qui ne sont pas compris dans les solutions de l'équation $\left(\frac{x}{c}\right)=1$, satisferont nécessairement à l'équation $\left(\frac{x}{c}\right)=-1$; et le nombre de ces derniers sera encore $\frac{c-1}{2}$; car le nombre des termes de la progression $1, 3, 5, 7 \ldots 2c-1$ étant $c$, si on exclut le terme $c$ qui ne satisfait ni à l'une ni à l'autre de ces équations, il restera $c-1$ termes dont la moitié satisfait à l'équation $\left(\frac{x}{c}\right)=1$, et l'autre à l'équation $\left(\frac{x}{c}\right)=-1$. Il est inutile d'ajouter que les solutions de cette dernière équation peuvent être aussi augmentées d'un multiple quelconque de $2c$.

(194) *Exemple I.* Soit $c=41$, on formera, au moyen des différences, la suite des quarrés impairs, et on retranchera, tant des différences

différences que des quarrés, les multiples de 82 à mesure qu'ils se présentent. Voici l'opération :

Differ. 8 16, 24 32 40, 48, 56, 64 72 80
Quar. 1, 9, 25, 49, 81, 121=39, 87=5, 61, 125=43, 115=33.

Differ. 88=6 14 22 30 38 46 54 62
Quar. 113=31, 37, 51, 73, 103=21, 59, 105=23, 77.

Differ. 70 78 86=4
Quar. 139=57, 127=45, 123=41=$c$.

Les 20 premiers termes rangés par ordre de grandeur, donneront la formule suivante, qui renferme toutes les solutions de l'équation $\left(\frac{x}{41}\right)=1$ :

$$x=82z+\begin{cases}1, & 5, \ 9, \ 21, \ 23, \ 25, \ 31, \ 33, \ 37, \ 39\\ 81, & 77, \ 73, \ 61, \ 59, \ 57, \ 51, \ 49, \ 45, \ 43.\end{cases}$$

On remarquera que les 20 valeurs numériques qui suivent $82z$, et qui sont proprement les solutions de l'équation proposée, sont telles que chaque valeur $b$ est accompagnée de son complément $2c-b$, les deux ensemble faisant constamment $2c$. C'est ce qui aura lieu généralement toutes les fois que le nombre $c$ sera de la forme $4m+1$; en effet si $b^{2m}-1$ est divisible par $c$, il est clair que $(2c-b)^{2m}-1$ est également divisible par $c$. Donc alors la solution ou racine $b$ est toujours accompagnée de la racine $2c-b$. Il n'en seroit pas de même, si $c$ étoit de la forme $4m-1$, et on voit, au contraire, que si $b$ satisfait à l'équation $\left(\frac{x}{c}\right)=1$, son complément $2c-b$ satisfera à l'équation $\left(\frac{x}{c}\right)=-1$.

(195) *Exemple II.* Soit $c=59$, $2c=118$, on procédera ainsi :

Differ. 8 16 24 32 40 48 56 64 72 80 88 96
Quar. 1, 9, 25, 49, 81, 121=3, 51, 107, 171=53, 125=7, 87, 175=57.

Differ. 104 112 120=2 10 18 26 34 42 50
Quar. 153=35, 139=21, 133=15, 17, 27, 45, 71, 105, 147=29.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Differ. | 58 | 66 | 74 | 82 | 90 | 98 | 106 | 114 |
| Quar. | 79, | 137=19, | 85, | 159=41, | 123=5, | 95, | 193=75, | 181=65. |

Rassemblant par ordre ces 29 résultats, on aura la formule suivante, qui contient toutes les solutions de l'équation $\left(\frac{x}{59}\right)=1$ :

$x=118z+$ 1, 3, 5, 7, 9; 15, 17, 19, 21, 25; 27, 29, 35, 41, 45;
49, 51, 53, 57, 63; 71, 75, 79, 81, 85; 87, 95, 105, 107.

Par conséquent les solutions de l'équation $\left(\frac{x}{59}\right)=-1$, seront:

$x=118z+$ 11, 13, 23, 31, 33; 37, 39, 43, 47, 55; 61, 65, 67, 69, 73;
77, 83, 89, 91, 93; 97, 99, 101, 103, 109; 111, 113, 115, 117.

## §. X. *Recherche des formes linéaires qui conviennent aux diviseurs de la formule* $t^2 + cu^2$.

Nous examinerons d'abord le cas où $c$ est un nombre premier, ce qui fournira deux théorêmes principaux.

(196) Théorème. *Soit* c *un nombre premier* $4n+1$, *et* A *un diviseur impair quelconque de la formule* $x^2 + c$ *ou* $t^2 + cu^2$, *je dis qu'on aura* $\left(\frac{A}{c}\right) = 1$ *si* A *est de la forme* $4n+1$, *et* $\left(\frac{A}{c}\right) = -1$ *si* A *est de la forme* $4n-1$.

Car soit $\alpha$ un nombre premier $4n+1$, et $\beta$ un nombre premier $4n-1$, tous deux diviseurs de $x^2+c$, on aura, suivant le n°. 134, $\left(\frac{-c}{\alpha}\right) = 1$ et $\left(\frac{-c}{\beta}\right) = 1$, ou $\left(\frac{c}{\alpha}\right) = 1$, et $\left(\frac{c}{\beta}\right) = -1$. De-là on conclut, par la loi de réciprocité, $\left(\frac{\alpha}{c}\right) = 1$, et $\left(\frac{\beta}{c}\right) = -1$. Mais le nombre $A$, s'il est de la forme $4n+1$, est le produit d'un nombre quelconque de facteurs $\alpha$ par un nombre pair de facteurs $\beta$, donc dans ce cas $\left(\frac{A}{c}\right) = 1$; et si le nombre $A$ est de la forme $4n-1$, il résulte du produit d'un nombre quelconque de facteurs $\alpha$ par un nombre impair de facteurs $\beta$, donc dans ce second cas on a $\left(\frac{A}{c}\right) = -1$.

*Corollaire.* Donc si on désigne par $b$ l'un des $\frac{c-1}{2}$ nombres impairs moindres que $2c$ qui satisfont à l'équation $\left(\frac{x}{c}\right) = 1$, on aura $A = 2cz + b$. Mais parmi les nombres $b$, on peut conserver ceux qui sont de la forme $4n+1$, et ajouter $2c$ à ceux qui sont de la forme $4n-1$; on aura par ce moyen $\frac{c-1}{2}$ nombres de

la forme $4n+1$, moindres que $4c$. Soit $a$ un de ces nombres, on aura $A=4cz+a$, ce qui donnera $\frac{c-1}{2}$ formes linéaires des diviseurs $4n+1$ de la formule $t^2+cu^2$.

Pareillement, si on réduit à la forme $4n-1$ toutes les solutions de l'équation $\left(\frac{x}{c}\right)=-1$, ce qui se fera, en conservant les nombres $4n-1$, et ajoutant $2c$ à ceux qui sont de la forme $4n+1$, on aura $\frac{c-1}{2}$ nombres de la forme $4n-1$, et moindres que $4c$; soit $a$ l'un quelconque de ces nombres, et l'expression $4cz+a$ sera la forme générale des diviseurs $4n-1$ de la formule $t^2+cu^2$.

Ainsi, par exemple, les diviseurs $4n+1$ de la formule $t^2+41u^2$ seront compris dans la formule

$$A=164z+1,5,9,21,25;33,37,45,49,57;61,73,77,81,105;113,121,125,133,141.$$

Et les diviseurs $4n-1$ de la même formule seront compris dans la formule

$$A=164z+3,7,11,15,19;27,35,47,55,63;67,71,75,79,95;99,111,135,147,151.$$

On conclura de-là, par voie d'exclusion, les diverses formes, soit $4n+1$, soit $4n-1$, qui ne divisent point $t^2+41u^2$. En général, il est aisé de voir qu'il y aura toujours autant de formes pour les non-diviseurs que pour les diviseurs, ce nombre étant égal à $\frac{c-1}{2}$ soit dans la forme $4n+1$, soit dans la forme $4n-1$.

*Remarque.* Tout nombre premier contenu dans les formes linéaires des diviseurs de $t^2+cu^2$ est nécessairement diviseur de $t^2+cu^2$. Car soit $A$ ce nombre premier, s'il est de la forme $4n+1$, on aura $\left(\frac{A}{c}\right)=1$, donc $\left(\frac{c}{A}\right)=1$, donc $A$ est diviseur de $t^2+cu^2$.

Si $A$ est de la forme $4n-1$, on aura $\left(\frac{A}{c}\right)=-1$, donc $\left(\frac{c}{A}\right)=-1$, donc $A$ est diviseur de $t^2+cu^2$.

Cette remarque est le fondement d'uu grand nombre de propriétés

des nombres premiers; car puisqu'étant donné $c$ on peut déterminer *a priori* toutes les *formes linéaires* $4cz+b$ dont sont susceptibles les diviseurs de la formule $t^2+cu^2$, et que d'un autre côté on peut aussi déterminer toutes les *formes quadratiques* $py^2+2qyz+rz^2$ qui conviennent à ces mêmes diviseurs, il s'ensuit que tout nombre premier renfermé dans l'une des formes linéaires $4cz+b$, doit être de l'une des formes quadratiques $py^2+2qyz+rz^2$. Proposition très-féconde, et dont le développement pour les différentes valeurs du nombre premier $c$, fournit une multitude de théorêmes intéressans sur les nombres premiers.

Lorsque $A$ est un nombre composé, il ne suffit pas qu'il soit compris dans les formes $4cz+b$ qui conviennent aux diviseurs de $t^2+cu^2$, et malgré cette condition, il pourroit bien n'être pas diviseur de cette formule. Par exemple, lorsque $c=41$, la forme $164z+57$ contient le nombre $221=13.17$, lequel n'est point diviseur de $t^2+41u^2$, car $t^2+41u^2$ n'est divisible ni par 13 ni par 17.

(197) Théorème. *Soit* c *un nombre premier* $4n-1$, *et* A *un diviseur impair quelconque de la formule* $t^2+cu^2$, *je dis qu'on aura toujours* $\left(\frac{A}{c}\right)=1$.

Car soit $\alpha$ un nombre premier $4n+1$, et $\mathcal{C}$ un nombre premier $4n-1$, tous deux diviseurs de $t^2+cu^2$, on aura $\left(\frac{-c}{\alpha}\right)=1$, $\left(\frac{-c}{\mathcal{C}}\right)=1$, ou $\left(\frac{c}{\alpha}\right)=1$, $\left(\frac{c}{\mathcal{C}}\right)=-1$; donc réciproquement $\left(\frac{\alpha}{c}\right)=1$, $\left(\frac{\mathcal{C}}{c}\right)=1$. Donc tout diviseur $A$ composé du produit de plusieurs nombres premiers $\alpha$ et $\mathcal{C}$, donnera $\left(\frac{A}{c}\right)=1$.

*Corollaire.* Tout diviseur impair de la formule $t^2+cu^2$, peut être représenté par $2cz+a$, $a$ étant l'un des $\frac{c-1}{2}$ nombres impairs et moindres que $2c$ qui satisfont à l'équation $\left(\frac{x}{c}\right)=1$.

Par exemple, si $c=59$, tout diviseur de la formule $t^2+59u^2$ pourra être représenté par la formule

$$A=118z+1, 3, 5, 7, 9; 15, 17, 19, 21, 25; 27, 29, 35, 41, 45; 49, 51, 53, 57, 63; 71, 75, 79, 81, 85; 87, 95, 105, 107.$$

On démontrera aussi, comme dans le cas précédent, que tout nombre premier compris dans la forme linéaire $2cz+a$ est nécessairement diviseur de $t^2+cu^2$.

*Remarque.* On trouveroit de même, à l'égard des diviseurs de la formule $t^2-cu^2$, les théorêmes suivans:

1°. Soit $c$ un nombre premier $4n+1$ et $A$ un diviseur impair quelconque de la formule $t^2-cu^2$, on aura $\left(\frac{A}{c}\right)=1$; donc $A$ sera toujours de la forme $2cz+\alpha$, $\alpha$ étant l'une des $\frac{c-1}{2}$ solutions de l'équation $\left(\frac{x}{c}\right)=1$, et réciproquement tout nombre premier compris dans les formes $2cz+\alpha$ sera diviseur de la formule $t^2-cu^2$.

2°. Soit $c$ un nombre premier $4n-1$ et $A$ un diviseur impair quelconque de la formule $t^2-cu^2$; si $A$ est de la forme $4n+1$, on aura $\left(\frac{A}{c}\right)=1$, et si $A$ est de la forme $4n-1$, on aura $\left(\frac{A}{c}\right)=-1$; de-là on tirera aisément les formes linéaires qui conviennent au diviseur $A$. Réciproquement tout nombre premier contenu dans ces formes sera diviseur de la formule $t^2-cu^2$.

(198) Considérons maintenant les diviseurs de la formule $t^2+2cu^2$, $c$ étant un nombre premier.

Soit d'abord $c=4n+1$, et soient $a$, $a'$, $a''$, $a'''$, des nombres premiers respectivement des formes $8m+1$, $8m+3$, $8m+5$, $8m+7$, tous diviseurs de $t^2+2cu^2$, on aura dans ces différens cas (n°. 134):

$$\left(\frac{2c}{a}\right)=1, \quad \left(\frac{2c}{a'}\right)=-1, \quad \left(\frac{2c}{a''}\right)=1, \quad \left(\frac{2c}{a'''}\right)=-1.$$

Mais on a en même temps (n°. 148)

$$\left(\frac{2}{a}\right)=1,\ \left(\frac{2}{a'}\right)=-1,\ \left(\frac{2}{a''}\right)=-1,\ \left(\frac{2}{a'''}\right)=1;$$

donc $\left(\frac{c}{a}\right)=1$, $\left(\frac{c}{a'}\right)=1$, $\left(\frac{c}{a''}\right)=-1$, $\left(\frac{c}{a'''}\right)=-1$, donc réciproquement $\left(\frac{a}{c}\right)=1$, $\left(\frac{a'}{c}\right)=1$, $\left(\frac{a''}{c}\right)=-1$, $\left(\frac{a'''}{c}\right)=-1$.

Soit maintenant $A$ un nombre quelconque de l'une des deux formes $8n+1$, $8n+3$, et soit $B$ un nombre de l'une des deux autres formes $8n+5$, $8n+7$; le nombre $A$ résultera nécessairement du produit d'un nombre quelconque de facteurs $a$, $a'$ par un nombre pair de facteurs $a''$, $a'''$, et ainsi on aura toujours $\left(\frac{A}{c}\right)=1$; de même le nombre $B$ résultera du produit d'un nombre quelconque de facteurs $a$, $a'$, par un nombre impair de facteurs $a''$, $a'''$, et ainsi on aura $\left(\frac{B}{c}\right)=-1$.

Soit en second lieu $c=4n-1$, et soient toujours $a$, $a'$, &c. des nombres premiers des formes $8n+1$, $8n+3$, &c. lesquels divisent la formule $t^2+2cu^2$, on aura, comme ci-dessus

$$\left(\frac{c}{a}\right)=1,\ \left(\frac{c}{a'}\right)=1,\ \left(\frac{c}{a''}\right)=-1,\ \left(\frac{c}{a'''}\right)=-1;$$

donc réciproquement $\left(\frac{a}{c}\right)=1$, $\left(\frac{a'}{c}\right)=-1$, $\left(\frac{a''}{c}\right)=-1$, $\left(\frac{a'''}{c}\right)=1$.

Soient $A$ et $B$ deux nombres composés, le premier $8n+1$ ou $8n+7$, le second $8n+3$ ou $8n+5$, il est aisé de voir que le nombre $A$ résulte du produit d'un nombre quelconque de facteurs $a$, $a'''$, par un nombre pair de facteurs $a'$, $a''$, et ainsi on aura toujours $\left(\frac{A}{c}\right)=1$. A l'égard du nombre $B$, il peut être censé formé du produit d'un nombre $A$ par l'un des facteurs $a'$, $a''$; donc on aura $\left(\frac{B}{c}\right)=-1$.

Nous pouvons donc établir ces deux théorêmes.

I. A *étant un diviseur quelconque* $8n+1$ *ou* $8n+3$, *et* B *un diviseur* $8n+5$ *ou* $8n+7$ *de la formule* $t^2+2cu^2$, *dans laquelle* c *est un nombre premier* $4n+1$, *on aura toujours* $\left(\frac{A}{c}\right)=1$ *et* $\left(\frac{\phantom{B}}{c}\right)=-1$.

II. A *étant un diviseur* $8n+1$ *ou* $8n+7$, *et* B *un diviseur* $8n+3$ *ou* $8n+5$ *de la formule* $t^2+2cu^2$ *dans laquelle* c *est un nombre premier* $4n-1$, *on aura toujours* $\left(\frac{A}{c}\right)=1$ *et* $\left(\frac{B}{c}\right)=-1$.

(199) De-là on voit qu'on peut déterminer *a priori* toutes les formes linéaires $8cx+b$ qui conviennent, soit aux diviseurs $\mathcal{A}$, soit aux diviseurs $B$ de la formule $t^2+2cu^2$.

Par exemple, soit $c=29$, les solutions de l'équation $\left(\frac{\mathcal{A}}{c}\right)=1$ étant

$\mathcal{A}=58z+1, 5, 7, 9, 13; 23, 25, 33, 35, 45; 49, 51, 53, 57,$

si on concilie ces solutions avec les formes $8n+1$ et $8n+3$, on aura toutes les formes des diviseurs $8n+1$, $8n+3$ de la formule $t^2+58u^2$, lesquelles sont :

$\mathcal{A}=232z+1, 9, 25, 33, 35; 49, 51, 57, 59, 65; 67, 81, 83, 91, 107;$
$115, 121, 123, 129, 139; 161, 169, 179, 187, 209; 219, 225, 227.$

On trouvera de même les formes des diviseurs $8n+5$, $8n+7$, de la même formule, lesquelles sont :

$B=232z+15, 21, 31, 37, 39; 47, 55, 61, 69, 77; 79, 85, 95, 101, 119;$
$127, 133, 135, 143, 157; 159, 189, 191, 205, 213; 215, 221. 229.$

Soit encore $c=11$, l'équation $\left(\frac{x}{11}\right)=1$ ayant pour solutions $x=22z+1, 3, 5, 9, 15$, si on ramène chaque solution aux formes $8n+1$ et $8n+7$, on aura toutes les formes des diviseurs $8n+1$ et $8n+7$ de la formule $t^2+22u^2$, lesquelles seront :

$\mathcal{A}=88z+1, 9, 15, 23, 25; 31, 47, 49, 71, 81.$

De même les solutions de l'équation $\left(\frac{x}{11}\right)=-1$ étant $x=22z+7$, $13, 17, 19, 21$, si on les réduit aux formes $8n+3$, $8n+5$, on aura

aura toutes les formes des diviseurs $8n+3$, $8n+5$ de la formule $t^2+22u^2$, lesquelles seront :

$$B = 88z + 13, 19, 21, 29, 35; 43, 51, 61, 83, 85.$$

(200) Ayant déterminé les diverses formes linéaires $8cx+b$ qui conviennent aux diviseurs de la formule $t^2+2cu^2$, on peut démontrer que tout nombre premier compris dans ces formes est nécessairement diviseur de $t^2+2cu^2$; car si, par exemple, $A$ est de la forme $8n+3$, et $c$ de la forme $4n+1$, on aura (n°. 198) $\left(\frac{A}{c}\right)=1$; de-là on déduit $\left(\frac{c}{A}\right)=1$; d'ailleurs on a, par la forme du nombre $A$, $\left(\frac{2}{A}\right)=-1$, donc $\left(\frac{-2c}{A}\right)=1$, donc $A$ est diviseur de $t^2+2cu^2$. Les autres cas se démontreront de la même manière.

*Remarque.* Il est essentiel d'observer que, quel que soit le nombre $c$, premier ou non, positif ou négatif, les diviseurs linéaires de la formule $t^2+cu^2$ seront les mêmes, soit qne ces diviseurs soient supposés des nombres premiers, soit qu'ils soient des nombres composés quelconques.

En effet, si on considère seulement parmi les diviseurs de la formule $t^2+cu^2$, ceux qui sont premiers à $c$ (et il est inutile d'en considérer d'autres, parce qu'on sait bien que tout diviseur de $c$ divisera la formule $t^2+cu^2$), et qu'on représente par $2cz+b$ l'nn des diviseurs linéaires dont il s'agit, $b$ sera premier par rapport à $c$, de sorte que la formule $2cz+b$ contiendra nécessairement des nombres premiers, et en contiendra même une infinité (Voyez l'Introd. n°. XXIV). Donc la forme $2cz+b$ sera comprise parmi toutes les formes possibles des nombres premiers qui divisent la formule $t^2+cu^2$; donc il suffit de chercher toutes les formes linéaires des diviseurs premiers, et celles-ci comprendront absolument toutes les formes possibles, tant des diviseurs simples qne des diviseurs composés.

Cette remarque abrégera singulièrement les calculs nécessaires pour déterminer *a priori* les formes linéaires des diviseurs de la formule $t^2+cu^2$, $c$ étant un nombre composé. Nous allons appliquer

cette méthode à quelques cas généraux; ensuite nous indiquerons une autre méthode moins directe, mais beaucoup plus expéditive pour remplir le même objet.

(201) Problème. *Soit* $c = \alpha\mathcal{C}$, $\alpha$ *et* $\mathcal{C}$ *étant des nombres premiers quelconques, 2 excepté, on demande quelle doit être la forme du nombre premier* A, *pour que* A *divise la formule* $t^2 + \alpha\mathcal{C}u^2$.

Il faut en général qu'on ait $\left(\frac{-\alpha\mathcal{C}}{A}\right) = 1$; mais pour satisfaire à cette équation, nous distinguerons deux cas, selon que $A$ est de la forme $4n+1$, ou de la forme $4n-1$.

1°. Si $A$ est un nombre premier $4n+1$, l'équation à résoudre sera $\left(\frac{\alpha}{A}\right)\cdot\left(\frac{\mathcal{C}}{A}\right) = 1$, et on n'y peut satisfaire que de deux manières, l'une en supposant $\left(\frac{\alpha}{A}\right) = 1$, $\left(\frac{\mathcal{C}}{A}\right) = 1$, l'autre en supposant $\left(\frac{\alpha}{A}\right) = -1$, $\left(\frac{\mathcal{C}}{A}\right) = -1$.

Dans le premier cas, on aura, par la loi de réciprocité, $\left(\frac{A}{\alpha}\right) = 1$, $\left(\frac{A}{\mathcal{C}}\right) = 1$. La première équation étant résolue, comme il a été expliqué ci-dessus, et les solutions étant toutes réduites à la forme $4n+1$, on aura $\frac{\alpha-1}{2}$ valeurs de $A$ de la forme $4\alpha z + \alpha'$; la seconde équation donnera pareillement $\frac{\mathcal{C}-1}{2}$ valeurs de $A$ de la forme $4\mathcal{C}z + \mathcal{C}'$. Donc si on fait accorder chacune des formules $4\alpha z + \alpha'$ avec chacune des formules $4\mathcal{C}z + \mathcal{C}'$, on aura en tout $\frac{\alpha-1}{2} \cdot \frac{\mathcal{C}-1}{2}$ formules de cette sorte $A = 4\alpha\mathcal{C}z + \gamma$.

Dans le second cas, on aura semblablement les équations $\left(\frac{A}{\alpha}\right) = -1$, $\left(\frac{A}{\mathcal{C}}\right) = -1$, lesquelles étant résolues séparément, puis combinées entr'elles, fourniront de même $\frac{\alpha-1}{2} \cdot \frac{\mathcal{C}-1}{2}$ formules de la forme $A = 4\alpha\mathcal{C}z + \gamma$.

2°. Si $A$ est un nombre premier $4n-1$, la condition à remplir sera $\left(\frac{\alpha\beta}{A}\right)=-1$, ou $\left(\frac{\alpha}{A}\right).\left(\frac{\beta}{A}\right)=-1$. On n'y peut satisfaire que de deux manières, soit en supposant $\left(\frac{\alpha}{A}\right)=1$, $\left(\frac{\beta}{A}\right)=-1$, soit en supposant $\left(\frac{\alpha}{A}\right)=-1$, $\left(\frac{\beta}{A}\right)=1$.

La première manière donne, d'après la loi de réciprocité, (n°. 164) $\left(\frac{A}{\alpha}\right)=(-1)^{\frac{\alpha+1}{2}}$, $\left(\frac{A}{\beta}\right)=(-1)^{\frac{\beta-1}{2}}$; et comme ces équations rentrent toujours dans l'une ou l'autre des deux équations $\left(\frac{x}{c}\right)=+1$, $\left(\frac{x}{c}\right)=-1$, $c$ étant un nombre premier, il sera facile d'avoir la valeur de $A$ qui satisfait à chacune de ces équations. Ensuite la combinaison des valeurs donnera un nombre $\frac{\alpha-1}{2}.\frac{\beta-1}{2}$ de solutions toutes de la forme $4\alpha\beta z+a$.

La seconde manière de satisfaire à la question, donnera $\left(\frac{A}{\alpha}\right)=(-1)^{\frac{\alpha-1}{2}}$, $\left(\frac{A}{\beta}\right)=(-1)^{\frac{\beta+1}{2}}$, et on en tirera des conséquences analogues. Il y aura donc en tout quatre formules générales $4\alpha\beta z+a$ contenant chacune pour (a) un nombre de valeurs $\frac{\alpha-1}{2}.\frac{\beta-1}{2}$.

(202) Si on suppose $c=\alpha\beta\gamma$, $\alpha$, $\beta$, $\gamma$ étant trois nombres premiers inégaux, 2 excepté, on s'y prendra d'une manière semblable pour trouver la forme des différens nombres premiers qui peuvent diviser la formule $t^2+cu^2$.

Soit $A$ l'un de ces nombres, il faudra en général qu'on ait $\left(\frac{-\alpha\beta\gamma}{A}\right)=1$. Supposons d'abord $A$ de la forme $4n+1$, cette équation deviendra $\left(\frac{\alpha}{A}\right).\left(\frac{\beta}{A}\right).\left(\frac{\gamma}{A}\right)=1$, et on ne pourra y satisfaire que de ces quatre manières :

1°. $\left(\frac{\alpha}{A}\right)=1$, $\left(\frac{\beta}{A}\right)=1$, $\left(\frac{\gamma}{A}\right)=1$

2°. $\left(\frac{\alpha}{A}\right)=1$, $\left(\frac{\beta}{A}\right)=-1$, $\left(\frac{\gamma}{A}\right)=-1$

3°. $\left(\frac{\alpha}{A}\right)=-1$, $\left(\frac{\beta}{A}\right)=1$, $\left(\frac{\gamma}{A}\right)=-1$

4°. $\left(\frac{\alpha}{A}\right)=-1$, $\left(\frac{\beta}{A}\right)=-1$, $\left(\frac{\gamma}{A}\right)=1$.

Dans le premier cas, on aura, par la loi de réciprocité, $\left(\frac{A}{\alpha}\right)=1$, $\left(\frac{A}{\beta}\right)=1$, $\left(\frac{A}{\gamma}\right)=1$; or les valeurs qui satisfont à ces équations sont de la forme $A=4\alpha z+\alpha'$, $A=4\beta z+\beta'$, $A=4\gamma z+\gamma'$, $\alpha'$ ayant $\frac{\alpha-1}{2}$ valeurs moindres que $4\alpha$, $\beta'$ ayant $\frac{\beta-1}{2}$ valeurs moindres que $4\beta$, et $\gamma'$ ayant $\frac{\gamma-1}{2}$ valeurs moindres que $4\gamma$. Donc si on fait accorder les trois valeurs $4\alpha z+\alpha'$, $4\beta z+\beta'$, $4\gamma z+\gamma'$, suivant toutes les combinaisons possibles, on aura une nouvelle formule $A=4\alpha\beta\gamma z+\omega$, dans laquelle $\omega$ aura un nombre de valeurs $\frac{\alpha-1}{2}\cdot\frac{\beta-1}{2}\cdot\frac{\gamma-1}{2}$.

Il y aura une formule semblable pour chacun des quatre cas qui sont à considérer lorsque $A$ est de la forme $4n+1$; il y en aura quatre pareilles pour représenter les valeurs de $A$ lorsque $A$ est de la forme $4n-1$. Donc on aura en tout huit formules, chacune renfermant $\frac{\alpha-1}{2}\cdot\frac{\beta-1}{2}\cdot\frac{\gamma-1}{2}$ formes différentes.

Il n'est pas difficile de voir que si $c$ contenoit un quatrième facteur $\delta$, le nombre des formules deviendroit double, et le nombre des formes contenues dans chacune seroit $\frac{\alpha-1}{2}\cdot\frac{\beta-1}{2}\cdot\frac{\gamma-1}{2}\cdot\frac{\delta-1}{2}$.

On peut donc établir cette conclusion générale.

*Si on désigne par* m *le nombre des facteurs premiers* $\alpha$, $\beta$, $\gamma$, &c. *qui composent le nombre* c, *les diviseurs impairs de la formule* $t^2+cu^2$ *seront représentés par* $2^m$ *formules* $A=4cz+a$, *dans cha-*

*cune desquelles* a *aura un nombre de valeurs* $\frac{\alpha-1}{2} \cdot \frac{6-1}{2} \cdot \frac{\gamma-1}{2} \cdot \frac{\delta-1}{2}$. &c., *de sorte que le nombre de toutes les formes linéaires contenues dans ces formules sera* $(\alpha-1)(6-1)(\gamma-1)$ &c.

Il pourra arriver que les formes $4n+1$, $4n-1$ soient confondues dans une même formule, laquelle seroit $2cz+a$, au lieu de $4cz+a$ que nous venons de trouver; mais alors il y auroit deux fois moins de formules, ce qui reviendroit au même.

(203) Si on a $c=2d$, $d$ étant un nombre impair résultant du produit des $m$ nombres premiers $\alpha$, $6$, $\gamma$, &c., il faudra considérer, à l'égard du diviseur $A$, les quatre formes $8n+1$, $8n+3$, $8n+5$, $8n+7$, chacune desquelles donne une valeur déterminée pour $\left(\frac{2}{A}\right)$, de sorte qu'il ne faudra plus que satisfaire à l'une ou l'autre des équations $\left(\frac{d}{A}\right)=1$, $\left(\frac{d}{A}\right)=-1$, selon les cas.

Cette équation, traitée toujours de la même manière, donnera $2^{m-1}$ valeurs de $A$, chacune de la forme $8dz+a$, dans laquelle (a) aura un nombre de valeurs $\frac{\alpha-1}{2} \cdot \frac{6-1}{2} \cdot \frac{\gamma-1}{2}$. &c. La même chose ayant lieu pour chacune des quatre formes $8n+1$, $8n+3$, &c., on aura donc en tout $2^{m+1}$ formules $A=8dz+a$, ou $A=4cz+a$, dans chacune desquelles (a) aura un nombre de valeurs $\frac{\alpha-1}{2} \cdot \frac{6-1}{2} \cdot \frac{\gamma-1}{2}$. &c., et le nombre total des formes linéaires sera par conséquent $2(\alpha-1)(6-1)(\gamma-1)$. &c.

Si le nombre $c$ contenoit un facteur quarré, on pourroit le diviser par ce facteur, car la formule $t^2+c\theta^2u^2$ n'est pas plus générale que $t^2+cu^2$, et n'admet pas d'autres diviseurs premiers à $c$. Ainsi on peut toujours supposer que $c$ est le produit de plusieurs nombres premiers inégaux, sans en excepter 2; de sorte que les deux cas généraux que nous venons d'examiner renferment absolument tous les cas possibles. Enfin, quoique nous n'ayons considéré jusqu'à

présent que le cas de $c$ positif, la formule $t^2 - cu^2$ se traiteroit de la même manière; et on auroit les mêmes résultats quant au nombre des formes $4cz + a$, qui conviennent aux diviseurs de cette formule. Mais dans tous les cas, on peut trouver ces différentes formes linéaires, par un procédé plus simple, et qui conduit à de nouvelles propriétés.

(204) On a déjà vu (n°. 138) que les différens diviseurs d'une formule telle que $t^2 \pm cu^2$ peuvent toujours se réduire à la forme

$$A = py^2 + 2qyz \pm rz^2,$$

dans laquelle on a $pr \mp q^2 = c$, et où l'on peut supposer $2q$ non plus grand que $p$ et $r$. Au moyen de ces conditions, il est facile de déterminer *a priori* toutes les formes des diviseurs qui répondent à un nombre donné $c$. Les formes $py^2 + 2qyz \pm rz^2$, contenant des indéterminées au second degré, seront appelées désormais *formes quadratiques*, pour les distinguer des formes linéaires $4cx + a$, dont nous nous sommes occupés dans ce paragraphe et dans le précédent.

Supposons donc qu'étant donné le nombre $c$ on a déterminé d'abord toutes les formes quadratiques qui conviennent aux diviseurs de la formule proposée $t^2 \pm cu^2$, il ne restera plus qu'à développer ces formes quadratiques en formes linéaires; on aura ainsi toutes les formes linéaires qui conviennent aux diviseurs de cette formule, on aura de plus l'avantage de connoître la correspondance qu'il y a entre les formes quadratiques et les formes linéaires.

Tout se réduit par conséquent à voir ce que devient la formule $py^2 + 2qyz \pm rz^2$, lorsqu'on y substitue, au lieu de $y$ et $z$, des nombres quelconques déterminés, et qu'on met les résultats sous la forme $4cx + a$, où l'on peut négliger les multiples de $4c$, et ne conserver que le résultat positif et moindre que $4c$.

Or il n'est pas nécessaire, dans cette substitution, de faire $y$ ni $z$ plus grands que $2c$; car si à la place de $y$ et $z$ on substitue $2c + y$ et $2c + z$, la formule $py^2 + 2qyz \pm rz^2$ deviendra

$$p(2c+y)^2 + 2q(2c+y)(2c+z) \pm r(2c+z)^2,$$

quantité qui se réduit à $py^2 + 2qyz \pm rz^2 + 4cM$, $4cM$ étant un

multiple de $4c$; de sorte que ces valeurs $2c+y$, $2c+z$ donneront la même forme linéaire $4cx+a$ qu'avoient donnée $y$ et $z$.

Il faut éviter également de donner à $y$ et $z$ des valeurs qui rendroient $py^2+2qyz\pm rz^2$ pair, car nous ne considérons ici que les diviseurs impairs, et de plus, les diviseurs premiers à $c$.

Pour remplir plus sûrement cette condition, il sera bon de préparer le diviseur quadratique $py^2+2qyz\pm rz^2$ de manière que $r$ soit pair, car alors $p$ étant impair, on donnera à $y$ des valeurs impaires quelconques, et à $z$ des valeurs paires ou impaires à volonté. Si $r$ n'est pas déjà pair dans le diviseur, il suffira de mettre $y\pm z$ à la place de $y$, et la transformée aura son dernier terme pair. Nous aurons occasion aussi, dans certains cas, de donner aux diviseurs quadratiques la forme $py^2+qyz+rz^2$ dans laquelle les trois coefficiens sont impairs. Alors il faudra supposer successivement $z=2u$, $y=2u$, $z+y=2u$, ce qui donnera trois formules ayant la condition requise; mais on verra que le développement d'une de ces formules suffit.

(205) Considérons donc la formule $A=py^2+2qyz\pm 2mz^2$, où l'on a $2mp\mp q^2=c$, et dans laquelle $y$ doit être impair, ainsi que $p$. Si on suppose $q$ et $c$ premiers entr'eux, $p$ et $c$ seront aussi premiers entr'eux. Cela posé, si l'on fait $y=1$, je dis que la formule $p+2q\psi\pm 2m\psi^2$, où il ne reste plus que $\psi$ d'indéterminé, contiendra toutes les formes linéaires $4cx+a$, qui sont comprises dans la formule proposée $py^2+2qyz\pm 2mz^2$.

Il faut prouver pour cela que, quelles que soient $y$ et $z$, on pourra toujours trouver une indéterminée $\psi$ telle que

$$\frac{p+2q\psi\pm 2m\psi^2-py^2-2qyz\mp 2mz^2}{4c}$$

soit un entier. En effet, puisque $p$ et $4c$ sont premiers entr'eux, la quantité précédente sera un entier, si son produit par $p$ en est un, c'est-à-dire si l'on a

$$\frac{(p+q\psi)^2-(py+qz)^2\pm c(\psi^2-z^2)}{4c}=e.$$

Soit d'abord $\psi=z+2\lambda$, et il suffira de satisfaire à la condition

$$\frac{(p+qz+2q\lambda)^2-(py+qz)^2}{4c}=e.$$

C'est ce qu'on peut obtenir, en prenant une nouvelle indéterminée $\theta$, telle que

$$p+qz+2q\lambda=py+qz+2c\theta;$$

or cette équation sera toujours résoluble, puisqu'elle peut être mise sous la forme

$$q\lambda-c\theta=p\left(\frac{y-1}{2}\right),$$

où $c$ et $q$ sont premiers entr'eux, et où d'ailleurs le second membre est un entier.

Donc pour déterminer toutes les formes linéaires de la formule $A=py^2+2qyz\pm 2mz^2$, il suffira de déterminer celles de la formule plus simple

$$A=p+2q\psi\pm 2m\psi^2;$$

ce qui se fera, en donnant à $\psi$ les valeurs successives 0, 1, 2, 3, &c. jusqu'à $2c-1$, ou seulement jusqu'à $c-1$ si $q=0$. Les valeurs de $A$ se calculent aisément par le moyen de leurs différences, et en omettant les multiples de $4c$ à mesure qu'ils se présentent. Ensuite on rejettera parmi tous les résultats ceux qui sont identiques avec d'autres, et ceux qui ont un commun diviseur avec $c$.

(206) Si $q$ et $c$ ne sont pas premiers entr'eux, il sera toujours facile de transformer la formule $py^2+2qyz\pm 2mz^2$ en une autre semblable, dans laquelle $q$ soit premier à $c$; de sorte qu'on doit regarder comme absolument général le procédé qu'on vient d'indiquer. Cependant nous dirons encore deux mots du cas particulier où la formule proposée est $y^2\pm cz^2$ ou $ay^2\pm bz^2$.

Si l'on a $A=y^2\pm cz^2$, il faudra distinguer deux cas, selon que $c$ est pair ou impair.

1°. Si $c$ est impair, on supposera d'abord $y$ impair et $z$ pair, ce qui, en rejetant les multiples de $4c$, réduit la valeur de $A$ au seul terme $y^2$, d'où résulte $A=1, 9, 25$, &c.; on supposera ensuite $y$ pair et $z$ impair, ce qui donnera $A=4u^2\pm c$, et ainsi on formera la suite $4\pm c$, $16\pm c$, $36\pm c$, &c., ayant toujours soin de rejeter les multiples de $4c$. Les résultats provenus de ces deux suppositions, composeront toutes les formes linéaires de $A$.

2°. Si $c$ est pair, il faudra nécessairement que $y$ soit impair, mais $z$ et

sera à volonté ; si $z$ est pair, on aura simplement $A=y^2=1, 9, 25$, &c. ; si $z$ est impair, on aura $A=y^2\pm c$ ; de sorte qu'il faudra former la suite $1\pm c$, $9\pm c$, $25\pm c$, &c. Les deux systèmes réunis donneront toutes les formes du diviseur $A$.

Si le nombre $c=ab$, parmi les diviseurs de $t^2\pm cu^2$, on rencontrera nécessairement $ay^2\pm bz^2$. Pour avoir les formes linéaires de ce diviseur, on donnera à $y$ les valeurs successives 1, 2, 3... jusqu'à $b-1$, et on donnera à $z$ les valeurs 1.2.3.... jusqu'à $a-1$. Il est inutile d'aller plus loin, parce que si à la place de $y$ on met $b+y$ et $b-y$, les deux résultats diffèrent d'un multiple de $4ab$ ou de $4c$, et par conséquent ne sont pas censés différens. Il en est de même, si on met $a+z$ et $a-z$ à la place de $z$. Il faudra donc combiner chacune des valeurs de $ay^2$ avec chacune des valeurs de $\pm bz^2$, et la seule condition que la somme soit un nombre impair, exclura beaucoup de combinaisons ; il faudra ensuite supprimer les résultats qui sont identiques avec d'autres, ou qui ont un commun diviseur avec $c$.

A ces préceptes généraux nous n'ajouterons plus qu'une observation, c'est que dans le cas de $c=4n-1$, les diviseurs linéaires de la formule $t^2+cu^2$ doivent être représentés simplement par $2cx+a$, au lieu de l'être par $4cx+a$, parce qu'alors une même forme quadratique contient les diviseurs $4n+1$ et les diviseurs $4n-1$. Le calcul d'ailleurs est toujours le même, avec cette seule différence, qu'au lieu de supprimer les multiples de $4c$, on supprime ceux de $2c$, ce qui rend l'opération encore plus prompte.

### EXEMPLE I.

(207) Soit proposé de trouver tous les diviseurs tant quadratiques que linéaires de la formule $t^2+41u^2$.

On cherchera d'abord les diviseurs quadratiques, au moyen de la formule $pr-q^2=41$, où l'on doit supposer $q<\sqrt{\frac{41}{3}}<4$, et $2q<p$ et $r$. Voici le calcul :

1°. Soit $q=0$, on aura $pr=41$, donc $p=1$, $r=41$.

2°. Soit $q=1$, on aura $pr=42$, donc $\begin{cases} p=3, & r=14 \\ p=7, & r=6 \\ p=21, & r=2 \end{cases}$

3°. Soit $q=2$, on aura $pr=45=5.9$, donc $p=5$, $r=9$.

4°. Soit $q=3$, on aura $pr=50$ ; mais 50 ne se décompose pas en deux facteurs plus grands que 6, ou dont le moindre soit égal à 6. Donc l'opération est terminée, et il n'y a que cinq formes possibles pour les diviseurs quadratiques de la formule proposée. De ces cinq formes, trois sont relatives aux diviseurs $4n+1$, savoir :

$$y^2+41z^2$$
$$21y^2+2yz+2z^2$$
$$5y^2+4yz+9z^2.$$

Les deux autres se rapportent aux diviseurs $4n-1$, et sont :

$$3y^2+2yz+14z^2$$
$$7y^2+2yz+6z^2.$$

Cherchons maintenant les formes linéaires qui répondent à ces formes quadratiques.

Prenons parmi les diviseurs $4n+1$ la forme $A=5y^2+4yz+9z^2$, et comme le coefficient du dernier terme est impair, mettons $y-z$ à la place de $y$, puis changeons le signe de $z$, nous aurons $A=5y^2+6yz+10z^2$. Après cette préparation, on peut considérer simplement la formule $A=5+6\psi+10\psi^2$. Voici les résultats que donne cette formule, en faisant successivement $\psi=0, 1, 2.3...$, et rejetant à mesure les multiples de $4c=164$.

Diff. 16 36 56 76 96 116 136 156 176=12
A = 5, 21, 57, 113, 189=25, 121, 237=73, 209=45, 201=37.
Diff. 32 52 72 92
A = 49, 81, 133, 205=41, 133.

Arrivé au résultat $41=c$, on voit que les précédens 133, 81, &c. doivent revenir dans l'ordre inverse de sorte qu'on parviendra ainsi au terme 5; mais il reste à savoir si, passé le terme 5, il n'y auroit pas de nouveaux termes non compris dans ceux qu'on a déjà trouvés. Pour cela, il faut prolonger la suite en arrière, comme on le voit ici :

Diff. —16, 4, 24, 44, 64 84 104 124 144 164=0
A = 21, 5, 9, 33, 77, 141, 225=61, 165=1, 125, 269=105.

Ici, à cause de la différence 0, nous n'irons pas plus loin, parce

que nous sommes sûrs maintenant que les termes précédens reviendront, et qu'on n'aura aucun nouveau terme. Donc en rassemblant les résultats trouvés, et excluant $41=c$, on aura les 20 formes suivantes qui répondent au diviseur proposé $5y^2+4yz+9z^2$, ou $5y^2+6yz+10z^2$; ces formes sont :

$$A=164x+1,\ 5,\ 9,\ 21,\ 25;\ 33,\ 37,\ 45,\ 49,\ 57;\ 61,\ 73,\ 77,\ 81,\ 105,\ 113,\ 121,\ 125,\ 133,\ 141.$$

Prenons maintenant la formule quadratique $A=y^2+41z^2$; en supposant d'abord $z$ pair, il suffira de développer la valeur $y^2$ d'où résulteront les mêmes 20 formes qu'on vient de trouver. Soit ensuite $y$ pair et $z$ impair, on aura à développer la valeur $A=4u^2+91$, de laquelle résulteront toujours les mêmes formes. Enfin la troisième forme quadratique $A=21y^2+2yz+2z^2$ des diviseurs $4n+1$ donne encore les mêmes formes, et en effet les formes trouvées comprennent toutes celles qui ont été déterminées *a priori* pour les diviseurs $4n+1$ de la formule $t^2+cu^2$, le développement des différentes formules ne pouvoit donc fournir d'autres formes que les 20 déjà trouvées n°. 196; mais on voit que chaque formule particulière les fournit toutes, et c'est une propriété que nous allons démontrer en général.

(208) *Si* c *est un nombre premier* $4n+1$, *les différens diviseurs quadratiques* $4n+1$ *de la formule* $t^2+cu^2$, *fourniront tous les mêmes formes linéaires* $4cz+a$, a *ayant* $\frac{c-1}{2}$ *valeurs positives moindres que* $4c$, *et ces valeurs ne seront autre chose que les solutions de l'équation* $\left(\frac{x}{c}\right)=1$ *réduites à la forme* $4n+1$. *Pareillement tous les diviseurs quadratiques* $4n-1$ *de la même formule fourniront les mêmes formes linéaires* $4cz+a$, a *ayant* $\frac{c-1}{2}$ *valeurs qui sont les solutions de l'équation* $\left(\frac{x}{c}\right)=-1$, *réduites à la forme* $4n-1$.

En effet soit $py^2+2qyz+2mz^2=A$ un diviseur $4n+1$ de la formule $t^2+cu^2$, $p$ étant par conséquent de la forme $4n+1$; il faut prouver que les formes linéaires tirées de cette formule coin-

cideront avec celles qui seroient tirées du diviseur $y^2+cz^2$ qui appartient pareillement à la forme $4n+1$. Changeons les indéterminées $y$ et $z$ de cette dernière formule en $\varphi$ et $\psi$, pour ne pas les confondre avec les autres, et la question est de faire voir que, quels que soient $y$ et $z$, on peut toujours déterminer $\varphi$ et $\psi$ de manière que la quantité

$$\frac{\varphi^2+c\psi^2-(py^2+2qyz+2mz^2)}{4c}$$

soit un entier; et puisque $p$ et $4c$ sont premiers entr'eux, cette quantité sera un entier, si son produit par $p$ en est un, ou si l'on a

$$\frac{p\varphi^2-(py+qz)^2+c(p\psi^2-z^2)}{4c}=e.$$

Or $p$ est de la forme $4n+1$, donc pourvu qu'on prenne $\psi=z$, ou seulement $\psi-z$ pair, $p\psi^2-z^2$ sera divisible par 4, et ainsi il ne restera plus qu'à satisfaire à l'équation

$$\frac{p\varphi^2-(py+qz)^2}{4c}=e.$$

Mais (n°. 196) le nombre $p$, comme diviseur $4n+1$ de $t^2+cu^2$, est tel que $\left(\frac{p}{c}\right)=1$; donc $c$ est diviseur de $x^2-p$, et par conséquent on peut trouver un nombre $\alpha$ tel que $\alpha^2-p$ soit divisible par $c$. Si on prend de plus $\alpha$ impair, $\frac{\alpha^2-p}{4c}$ sera un entier; donc l'équation à laquelle on veut satisfaire deviendra

$$\frac{\alpha^2\varphi^2-(py+qz)^2}{4c}=e.$$

Cette équation est toujours résoluble, puisque $\alpha$ et $2c$ étant premiers entr'eux, on peut toujours trouver deux indéterminées $\varphi$ et $\theta$ telles que

$$\alpha\varphi-(py+qz)=2c\theta.$$

Donc il n'est aucune forme linéaire contenue dans le diviseur quadratique $py^2+2qyz+2mz^2$ qui ne soit pareillement contenue dans le diviseur $y^2+cz^2$, et la proposition réciproque se prouveroit par un raisonnement semblable. Or la forme $y^2+cz^2$ renferme toutes les formes linéaires possibles, puisqu'en faisant $z$ pair, elle

se réduit à $y^2$ qui les renferme toutes (n°. 193) ; donc toutes ces formes sont pareillement contenues dans le diviseur quadratique $py^2+2qyz+2mz^2$.

On démontrera la même chose de deux diviseurs quadratiques $4n-1$, représentés par $py^2+2qyz+2mz^2$ et $p'y'^2+2q'y'z'+2m'z'^2$. D'où il suit que dans le cas où $c$ est un nombre premier $4n+1$, tous les diviseurs quadratiques $4n+1$, donnent les mêmes formes linéaires, et il suffit par conséquent de développer le premier diviseur quadratique $y^2+cz^2$, ou simplement $y^2$ ; dans ce même cas, tous les diviseurs quadratiques $4n-1$ fournissent pareillement les mêmes formes linéaires, de sorte qu'il suffit de développer l'un de ces diviseurs.

(209) *Soit maintenant* c *un nombre premier* $4n-1$, *je dis que tout diviseur quadratique* $py^2+2qyz+rz^2$ *de la formule* $t^2+cu^2$, *contiendra les mêmes formes linéaires que donne le diviseur* $y^2+cz^2$, *ces formes linéaires étant représentées par la formule* $2cx+a$.

Il suffit, pour cela, de prouver que quels que soient $y$ et $z$, on peut toujours déterminer $\varphi$ et $\psi$ de manière que la quantité

$$\frac{\varphi^2+c\psi^2-(py^2+2qyz+rz^2)}{2c}$$

soit un entier. Or comme $p$ et $2c$ sont premiers entr'eux, si on multiplie cette quantité par $p$, on aura l'équation à résoudre

$$\frac{p\varphi^2-(py+qz)^2+c(p\psi^2-z^2)}{2c}=e;$$

et d'abord en prenant $\psi-z$ pair, $p\psi^2-z^2$ sera toujours divisible par 2, et ainsi il suffira de satisfaire à l'équation

$$\frac{p\varphi^2-(py+qz)^2}{2c}=e.$$

Mais $p$ étant un diviseur de $t^2+cu^2$, on a (n°. 197) $\left(\frac{p}{c}\right)=1$ ; donc $c$ est diviseur de $t^2-p$, et ainsi on peut supposer $\frac{a^2-p}{2c}=e$, et l'équation à résoudre deviendra

$$\frac{a^2\varphi^2-(py+qz)^2}{2c}=e.$$

Or on satisfait à cette équation, en cherchant les indéterminées $\varphi$ et $\theta$ telles que

$$\alpha\varphi-(py+qz)=2c\theta;$$

équation toujours résoluble, puisque $\alpha$ et $2c$ sont premiers entr'eux. Donc les formes linéaires contenues dans le diviseur quadratique $py^2+2qyz+rz^2$, sont également contenues dans le diviseur $y^2+cz^2$, et comme la propriété réciproque se démontreroit de la même manière, il suit de toutes deux qu'un diviseur quadratique quelconque $py^2+2qyz+rz^2$ renferme absolument toutes les formes linéaires qui conviennent aux diviseurs de la formule $t^2+cu^2$. Donc lorsque $c$ est un nombre premier $4n-1$, les mêmes formes linéaires sont affectées à la totalité des diviseurs quadratiques et à chacun d'eux en particulier.

On verra qu'il n'en est pas de même, lorsque $c$ est un nombre composé : alors les formes linéaires sont distinguées en plusieurs groupes qui répondent à différens systêmes de diviseurs quadratiques. L'existence de ces groupes est d'ailleurs une suite de ce qui a été démontré *a priori* sur la forme linéaire des diviseurs.

EXEMPLE II.

(210) On demande les diviseurs linéaires de la formule $t^2-39u^2$ avec les diviseurs quadratiques correspondans.

Pour cela, on commencera par chercher tous les diviseurs quadratiques, d'après la formule $pr+q^2=39$, où l'on peut donner à $q$ toutes les valeurs moindres que $\sqrt{\frac{39}{4}}$ ou $<3$; ces diviseurs sont

$$\begin{array}{ll} y^2-39z^2 & 39y^2-z^2 \\ 3y^2-13z^2 & 13y^2-3z^2 \\ 19y^2+2yz-2z^2 & 2y^2-2yz-19z^2 \\ 5y^2+4yz-7z^2 & 7y^2-4yz-5z^2. \end{array}$$

Mais en suivant la méthode pour réduire ces diviseurs au moindre nombre possible, on trouve qu'il ne reste que les quatre suivans ;

$$\begin{array}{ll} y^2-39z^2 & 39y^2-z^2 \\ 19y^2+2yz-2z^2 & 2y^2-2yz-19z^2. \end{array}$$

Il s'agit donc d'avoir les formes linéaires qui répondent à ces formes quadratiques.

1°. Le diviseur $y^2 - 39z^2$, en supposant $z$ pair et négligeant toujours les multiples de $4.39 = 156$, se réduit au seul terme $y^2$ dont voici les valeurs successives :

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Différ. | 8, | 16, | 24, | 32, | 40, | 48, | 56, | 64, | 72, | 80, | 88, | 96, | |
| $y^2$ | 1, | 9, | 25, | 49, | 81, | 121, | 13, | 69, | 133, | 49, | 129, | 61. | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Différ. | 104, | 112, | 120, | 128, | 136, | 144, | 152, | 4, | 12, | |
| $y^2$ | 1, | 105, | 61, | 25, | 153, | 133, | 121, | 117, | 121, | &c. |

Supprimant dans cette suite les termes divisibles par 3 et par 13, il ne restera que six termes différens, 1, 25, 49, 61, 121, 133; de sorte que le diviseur quadratique $y^2 - 39z^2$ comprend les formes linéaires

$$156x + 1,\ 25,\ 49,\ 61,\ 121,\ 133.$$

Il suffit de changer les signes des nombres déterminés, ou d'en prendre le complément à 156, et on aura les formes linéaires qui répondent au diviseur $39y^2 - z^2$; ces formes seront donc

$$156x + 23,\ 35,\ 95,\ 107,\ 131,\ 155.$$

Venons à l'une des deux autres formes $19y^2 + 2yz - 2z^2$, il suffira de développer la formule $19 + 2\psi - 2\psi^2$, d'où l'on déduira les résultats suivans :

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Différ. | 0 | −4 | −8 | −12 | −16 | −20 | −24 | −28 | −32 | −36 |
| Suite. | 19, | 19, | 15, | 7, | −5=151, | 135, | 115, | 91, | 63, | 31. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Différ. | −40 | −44 | −48 | −52 | −56 | −60 | −64 | −68 |
| Suite. | −5=151, | 111, | 67, | 19, | −33=123, | 67, | 7, | −57=99. |

| | | | | |
|---|---|---|---|---|
| Différ. | −72 | −76 | −80 | |
| Suite. | 31, | −41=115, | 39, | −41, &c. |

Écartant les termes répétés et ceux qui sont divisibles par 3 ou par 13, il ne restera encore que six nombres, d'où l'on conclura que la forme quadratique $19y^2 + 2yz - 2z^2$ comprend les six formes linéaires

$$156x + 7,\ 19,\ 31,\ 67,\ 115,\ 151.$$

Le complément de celles-ci donnera les formes linéaires qui répondent à l'autre forme quadratique $2y^2 - 2yz - 19z^2$, et qui seront

$$156x + 5,\ 41,\ 89,\ 125,\ 137,\ 149.$$

Nous avons donc dans cet exemple quatre groupes de diviseurs linéaires, chacun composé de six formes, et chacun répondant à un diviseur quadratique de la même formule. C'est ce qui s'accorde avec la théorie générale donnée ci dessus, en vertu de laquelle, si le nombre $c$ est le produit de deux nombres premiers $\alpha$, $6$, le système entier des diviseurs linéaires doit se décomposer en $2^2$ groupes, chacun composé de $\frac{\alpha-1}{2} \cdot \frac{6-1}{2}$ termes; en effet, dans ce cas, $\alpha=3$, $6=13$, et $\frac{3-1}{2} \cdot \frac{13-1}{2}=6$: aussi chaque groupe est-il composé de six termes.

EXEMPLE III.

(211) La formule $t^2+105u^2$ ayant pour l'un de ses diviseurs $5y^2+21z^2$, on demande les formes linéaires qui répondent à ce diviseur quadratique.

Prenons d'abord $y$ impair et $z$ pair, le terme $5y^2$ développé seul, en négligeant les multiples de $4c$ ou de 420, donne une suite qui se réduit aux sept termes 5, 45, 125, 185, 245, 285, 405; l'autre terme $21z^2$, où $z$ doit être pair, ne donne que les deux termes 84, 336. Il faut donc aux sept termes précédens, ajouter 84 ou 336, ce qui donnera les quatorze termes:

$$\begin{array}{ccccccc} 89, & 129, & 209, & 269, & 329, & 369, & 69, \\ 341, & 381, & 41, & 101, & 161, & 201, & 321, \end{array}$$

desquels retranchant ceux qui ont un commun diviseur avec 105, il ne restera que les six termes 41, 89, 101, 209, 269, 341.

On trouveroit absolument les mêmes six termes, si dans le diviseur $5y^2+21z^2$, on supposoit $z$ impair et $y$ pair, ainsi il n'y a que six formes linéaires qui répondent au diviseur $5y^2+21z^2$, savoir:

$$420x+41,\ 89,\ 101,\ 209,\ 269,\ 341.$$

EXEMPLE IV.

(212) La même formule $t^2+105u^2$ a pour diviseur quadratique $13y^2+10yz+10z^2$; mais comme dans ce diviseur $q=5$, et que 5 est diviseur de 105, on ne peut donner au diviseur quadratique la forme $13+10\psi+10\psi^2$, parce que le résultat en seroit incomplet. Il faut donc, par une substitution (n°. 206), faire en sorte que

que le terme moyen de la formule n'ait plus de commun facteur avec 105 ; or on trouve bientôt qu'en mettant $y+2z$ au lieu de $y$, on a la transformée $13y^2+62yz+82z^2$, laquelle a la condition requise. Il reste donc maintenant à développer la formule $13+62\psi+82\psi^2$; en voici le calcul :

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Differ. | 144 | 308 | 52 | 216 | 380 | 124 | 288 | 32 | 196 | 360 |
| Suite. | 13, | 157, | 45, | 97, | 313, | 273, | 397, | 265, | 297, | 73; |

et il est inutile de le prolonger plus loin, parce qu'il fournit six termes distincts; ainsi les formes linéaires qui répondent au diviseur quadratique $13y^2+10yz+10z^2$ sont :

$$420x+13,\ 73,\ 97,\ 157,\ 313,\ 397.$$

Voici, au reste, le système entier des diviseurs quadratiques de $t^2+105u^2$ avec les formes linéaires correspondantes.

| *Diviseurs quadratiques.* | *Diviseurs linéaires correspondans.* |
|---|---|
| $y^2+105z^2$ | $420x+1$, 109, 121, 169, 289, 361 |
| $53y^2+2yz+2z^2$ | $420x+53$, 113, 137, 197, 233, 317 |
| $5y^2+21z^2$ | $420x+41$, 89, 101, 209, 269, 341 |
| $13y^2+10yz+10z^2$ | $420x+13$, 73, 97, 157, 313, 397 |
| $3y^2+35z^2$ | $420x+47$, 83, 143, 167, 227, 383 |
| $19y^2+6yz+6z^2$ | $420x+19$, 31, 139, 199, 271, 391 |
| $7y^2+15z^2$ | $420x+43$, 67, 127, 163, 247, 403 |
| $11y^2+14yz+14z^2$ | $420x+11$, 71, 179, 191, 239, 359 |

Il y a donc en tout huit groupes de diviseurs linéaires composés chacun de six termes. Et en effet, suivant la théorie donnée ci-dessus (n°. 202), le nombre 105 étant 3.5.7, il doit y avoir $2^3$ groupes composés chacun du nombre de termes $\frac{3-1}{2}\cdot\frac{5-1}{2}\cdot\frac{7-1}{2}=6$. Nous voyons de plus, dans ce développement, que chaque groupe répond à un diviseur quadratique, et ne répond qu'à un seul.

## §. XI. *Explication des Tables III, IV, V, VI, et VII.*

### TABLE III.

(213) La Table III contient tous les diviseurs quadratiques de la formule $t^2-cu^2$, et les diviseurs linéaires correspondans; elle est calculée, pour tous les nombres depuis $c=2$ jusqu'à $c=79$, excepté les nombres quarrés ou divisibles par un quarré. On a exclu ceux-ci, parce que les diviseurs de la formule $t^2-c\theta^2u^2$, en les supposant premiers à $c\theta^2$, sont les mêmes que ceux de la formule $t^2-cu^2$.

Les diviseurs quadratiques représentés généralement par la formule $py^2+2qyz-rz^2$, où l'on a $pr+q^2=c$, sont réduits au moindre nombre possible par la méthode du §. XIII.

Tout diviseur quadratique $py^2+2qyz-rz^2$ doit être accompagné de son inverse $ry^2+2qyz-pz^2$. Mais ces deux formes sont quelqnefois identiques l'une avec l'autre, et cela arrive lorsqu'on peut satisfaire à l'équation $m^2-cn^2=-1$ (voy. n°. 90). Dans ces cas, on n'a mis dans la table que l'une des deux formes qui doivent être identiqnes.

A côté de chaque diviseur quadratique, on a mis les diviseurs linéaires qui en résultent, calculés suivant la méthode du §. précédent. Ces diviseurs sont toujours supposés premiers au nombre $c$, et on ne considère que les diviseurs impairs, quoique les formules $py^2+2qyz-rz^2$ renferment aussi des nombres pairs.

On observe constamment dans cette Table, que les diviseurs linéaires se partagent en plusieurs groupes dont le nombre, ainsi que la quantité de termes contenus dans chacun, sont conformes à la loi générale (n°. 203). Cependant il arrive quelquefois que deux de ces groupes sont réunis pour répondre à une même forme quadratique. Ainsi, lorsque $c=66=2.3.11$, la proposition générale dit qu'il y a $2^3$ ou 8 groupes composés chacun de $\frac{3-1}{2}\cdot\frac{11-1}{2}$

ou 5 termes ; mais on ne trouve dans la Table que quatre groupes composés de 10 termes, ce qui a eu lieu par la réunion de deux groupes en un seul. D'ailleurs le nombre total des formes linéaires est toujours 40, comme il doit être suivant la théorie.

## TABLE IV.

(214) La Table IV contient les diviseurs tant quadratiques que linéaires de la formule $t^2+au^2$, pour tout nombre $a$ de forme $4n+1$, non quarré ni divisible par un quarré, depuis 1 jusqu'à 105.

La première formule $t^2+u^2$ qui n'a qu'un seul diviseur quadratique $y^2+z^2$, n'a aussi que le seul diviseur linéaire $4x+1$. Toutes les autres formules $t^2+5u^2$, $t^2+13u^2$, &c. admettent à-la-fois des diviseurs $4n+1$ et des diviseurs $4n-1$; il est même à remarquer 1°. que les diviseurs quadratiques qui contiennent les nombres $4n+1$ sont toujours distincts de ceux qui contiennent les nombres $4n-1$; 2°. qu'il y a toujours autant de formes linéaires pour les diviseurs $4n+1$ qu'il y en a pour les diviseurs $4n-1$. Il n'en est pas toujours de même des formes quadratiques. On voit, par exemple, que la formule $t^2+41u^2$ a trois diviseurs quadratiques $4n+1$, et seulement deux $4n-1$. De même la formule $t^2+65u^2$ en a quatre de la première espèce, et deux seulement de la secoude.

(215) On a apporté dans cette Table une légère modification à la forme générale des diviseurs quadratiques $py^2+2qyz+rz^2$; elle consiste en ce qu'on a supposé constamment $q$ impair. Par ce moyen, $q^2+a$ ou $pr$ étant un nombre pair, on peut mettre $2m$ à la place de $r$, et la forme des diviseurs quadratiques devient $py^2+2qyz+2mz^2$, dans laquelle les nombres $p$ et $m$ seront toujours impairs.

Cette forme a l'avantage d'en fournir immédiatement une autre $2py^2+2qyz+mz^2$, et ces deux formes, à cause de la liaison qu'elles ont entr'elles, s'appelleront désormais *formes conjuguées*, ou *diviseurs conjugués.*

Nous avons dit que les nombres $p$ et $m$ sont toujours impairs ; en effet $q^2$ étant de la forme $8n+1$, et $a$ de la forme $4n+1$, il est clair que $q^2+a$ ou $2pm$ sera de la forme $4n+2$, donc $pm$ sera

nécessairement impair. Mais il faut distinguer deux cas selon que $a$ est de la forme $8n+1$ ou $8n+5$.

1°. Si $a$ est de la forme $8n+1$, alors $q^2+a$ sera de la forme $8n+2$ et $pm$ de la forme $4n+1$, ce qui ne peut avoir lieu, à moins que les nombres $p$ et $m$ ne soient tous deux de la forme $4n+1$, ou tous deux de la forme $4n-1$; donc alors les formes conjuguées $py^2+2qyz+2mz^2$, $2py^2+2qyz+mz^2$ appartiennent toutes deux aux diviseurs $4n+1$, ou toutes deux aux diviseurs $4n-1$.

2°. Si $a$ est de la forme $8n+5$, $pm$ sera de la forme $4n+3$, de sorte que les deux nombres $p$ et $m$ seront, l'un de forme $4n+1$, l'autre de forme $4n-1$. Donc alors les deux formes conjuguées appartiennent, l'une aux diviseurs $4n+1$, l'autre aux diviseurs $4n-1$. De-là on voit que a *étant un nombre quelconque* 8n+5, *la formule* $t^2+au^2$ *aura toujours autant de diviseurs quadratiques* $4n+1$ *que de diviseurs quadratiques* $4n-1$.

(216) Les diviseurs quadratiques de la formule $t^2+au^2$ étant trouvés par la méthode générale, il sera toujours facile de les réduire à la forme $py^2+2qyz+2mz^2$, où $q$ est impair; car il n'y aura à transformer que ceux où $q$ seroit pair, et dans ceux-ci il suffira de mettre $y-z$ à la place de $y$.

On peut aussi trouver directement tous les diviseurs quadratiques d'une formule donnée $t^2+au^2$, réduits à la forme $py^2+2qyz+2mz^2$. Pour cela, il faut observer qu'en laissant $q$ impair, on peut toujours faire en sorte que $q$ n'excède ni $p$ ni $m$. Car en substituant $y-2\alpha z$ à la place de $y$, si on a $q>p$, ou $z-\alpha y$ à la place de $z$, si on a $q>m$, on déterminera aisément le nombre $\alpha$ de manière qu'on ait dans la transformée $q<p$, ou $q<m$. Donc par une ou plusieurs substitutions de cette sorte, toute formule $py^2+2qyz+2mz^2$, dans laquelle $2pm-q^2=a$ pourra être ramenée à une formule semblable, où $q$ n'excédera ni $p$ ni $m$, de sorte qu'on aura $2pm-q^2>q^2$, et par conséquent $q<\sqrt{a}$.

Donc pour avoir toutes les formes quadratiques $py^2+2qyz+2mz^2$ qui conviennent aux diviseurs de la formule $t^2+au^2$, il faut donner à $q$ les valeurs impaires successives $1, 3, 5\ldots$ jusqu'à $\sqrt{a}$. Chaque

valeur de $q$ en donnera une pour $pm = \frac{q^2+a}{2}$ ; et si cette valeur peut se décomposer en deux facteurs $p$ et $m$ non moindres que $q$, il en résultera les deux diviseurs conjugués $py^2+2qyz+2mz^2$, $2py^2+2qyz+mz^2$.

Cette méthode donnera, comme la méthode générale, toutes les formes possibles des diviseurs quadratiques ; elle est plus expéditive, en ce qu'on n'a à essayer que les valeurs de $q$ impaires, et plus petites que $\sqrt{a}$, tandis que par la méthode générale on doit essayer toutes les valeurs de $q$ paires ou impaires jusqu'à $\sqrt{\frac{1}{3}a}$ ; or on a $\frac{1}{2}\sqrt{a} < \sqrt{\frac{1}{3}a}$.

Suivant cette nouvelle méthode, le diviseur quadratique $y^2+az^2$ est représenté par la formule $y^2+2yz+(a+1)z^2$, et son conjugué est $2y^2+2yz+\left(\frac{a+1}{2}\right)z^2$. On a laissé dans la Table, pour plus d'uniformité, la forme $y^2+2yz+(a+1)z^2$, excepté dans la première case où l'on n'a pas voulu altérer la simplicité du diviseur $y^2+z^2$ en mettant à sa place $y^2+2yz+2z^2$.

Dans tous les cas, les formes linéaires ont été conclues des formes quadratiques par les méthodes du §. précédent, et le nombre des groupes, ainsi que des termes contenus dans chacun, est toujours conforme à la loi générale.

## TABLE V.

(217) La Table V contient les diviseurs tant quadratiques que linéaires de la formule $t^2+au^2$, $a$ étant un nombre $4n-1$ non quarré, ni divisible par un quarré.

Les diviseurs quadratiques sont restés sous leur forme ordinaire, lorsque $a=8n+7$, mais ils ont subi une modification, lorsque $a=8n+3$. C'est ce que nous allons expliquer.

Si $a$ est de la forme $8n+3$, et qu'on désigne par $P$ un diviseur quelconque impair de la formule $t^2+au^2$, on pourra toujours supposer $t$ et $u$ impairs, et alors $t^2+au^2$ étant de la forme $8n+4$, le quotient de $t^2+au^2$ divisé par $P$ sera nécessairement de la même forme $8n+4$, ou $4p$, $p$ étant un nombre impair : on aura donc

$$t^2+au^2=4Pp.$$

Dans cette équation, les nombres $u$ et $2p$ sont premiers entre eux ; car s'ils avoient un commun diviseur, $t$ et $u$ en auroient un aussi, ce qui est contre la supposition ; donc on peut faire $u=z$ et $t=2py+qz$, ce qui donnera

$$P=py^2+qyz+\frac{q^2+a}{4p}z^2.$$

Or cette équation ne pent subsister, à moins que $\frac{q^2+a}{4p}$ ne soit un entier ; soit donc $q^2+a=4pr$, et on aura

$$P=py^2+qyz+rz^2.$$

Dans cette formule, il est aisé de voir que les trois coefficiens $p$, $q$, $r$ sont impairs ; car d'abord puisque $t$ est impair, et qu'on a $t=2py+qz$, il est clair que $q$ est impair ; ensuite $q^2$ étant de la forme $8n+1$, et $a$ de la forme $8n+3$, $q^2+a$ est de la forme $8n+4$ ; donc $\frac{q^2+a}{4}$ on $pr$ est impair ; donc $p$ et $r$ sont impairs.

De-là on voit que tout diviseur impair de la formnle $t^2+au^2$ peut toujours être réduit à la forme $py^2+qyz+rz^2$ où l'on a $p$, $q$, $r$ impairs et $4pr-q^2=a$. Je dis de plus, que dans cette formule on pourra supposer le coefficient moyen $q$ plus petit, ou au moins non plus grand qne chacun des extrêmes $p$ et $r$ ; en effet si on avoit, par exemple, $q>p$, on mettroit $y-\alpha z$ à la place de $y$, et le coefficient moyen devenant $q-2\alpha p$, on pourroit, au moyen de l'indéterminée $\alpha$, rendre ce coefficient plus petit ou au moins non plus grand que $p$.

Puis donc qne $p$ et $r$ sont plus grands ou non moindres que $q$, il est clair que $4pr-q^2$ sera $>3q^2$, et qu'ainsi on aura $q<\sqrt{\frac{a}{3}}$.

Donc pour avoir toutes les formes quadratiques qui conviennent aux diviseurs impairs de la formule $t^2+au^2$, il faudra donner à $q$ les valeurs impaires successives 1, 3, 5 jusqu'à $\sqrt{\frac{a}{3}}$ : chaque valeur de $q$ en donnera une pour $pr=\frac{q^2+a}{4}$, et si cette valeur peut se décomposer en deux facteurs non moindres que $q$, il en résultera une des formes quadratiques demandées.

(218) Soit, par exemple, $a=91$, si l'on fait $q=1$ on a $\frac{q^2+a}{4}=23=1.23$, d'où résulte le diviseur $y^2+yz+23z^2$.

Si l'on fait $q=3$, on a $\frac{q^2+a}{4}=25=5.5$, d'où résulte un second diviseur $5y^2+3yz+5z^2$.

La limite de $q$ étant $\sqrt{\frac{91}{3}}$ on peut faire encore $q=5$, ce qui donnera $\frac{q^2+a}{4}=29$. Mais ce nombre étant premier, il n'en résulte aucun nouveau diviseur. Donc les deux formules trouvées sont les seuls diviseurs quadratiques de $t^2+91u^2$.

Soit encore $a=163$, la limite de $q$ étant $\sqrt{\frac{163}{3}}<9$, on pourra faire successivement $q=1, 3, 5, 7$, d'où résultera $pr=41, 43, 47, 53$; mais ces nombres étant premiers, il s'ensuit que la formule $t^2+163u^2$ ne peut avoir que le seul diviseur quadratique $y^2+yz+41z^2$.

(219) La formule $py^2+qyz+rz^2$, dont les coefficiens sont impairs, représente en général trois diviseurs quadratiques de forme ordinaire où le coefficient moyen est pair; car dans l'application de cette formule, il faudra prendre les nombres $y$ et $z$ tous deux impairs, ou l'un pair, l'autre impair; on ne pourra donc faire que les trois suppositions $z=2u$, $y=2u$, $y=2u-z$, lesquelles donneront les trois formes

$$py^2+2qyu+4ru^2$$
$$4pu^2+2qzu+rz^2$$
$$4pu^2+(2q-4p)uz+(p-q+r)z^2.$$

Ces trois formes se réduisent à deux, lorsque deux des nombres $p$, $q$, $r$ sont égaux. Elles se réduisent à une seule, si les trois nombres $p$, $q$, $r$ sont égaux entr'eux; mais ce cas n'a lieu que lorsqu'ils sont égaux à l'unité, ou lorsque la formule proposée est $t^2+3u^2$, et alors le diviseur $y^2+yz+z^2$ se réduit à la seule forme $y^2+3z^2$, comme nous l'avons déjà trouvé (n°. 141). Dans tout autre cas, les trois formules qu'on vient de développer seront

essentiellement différentes les unes des autres. Il suit de-là qu'on diminue beaucoup le nombre des diviseurs quadratiques en les représentant par la formule à coefficiens impairs $py^2+qyz+rz^2$; il est d'ailleurs facile, ainsi qu'on vient de le voir, de développer ces diviseurs à coefficiens impairs en diviseurs quadratiques de forme ordinaire, ce qui en donnera un nombre à-peu-près triple.

(220) Il est utile d'observer que les diviseurs quadratiques compris dans la Table V, tant pour le cas de $a=8n+3$, que pour celui de $a=8n+7$, peuvent toujours être ramenés à la forme $py^2+4\varphi yz+\pi z^2$, laquelle ne diffère de la forme générale $py^2+2qyz+rz^2$, qu'en ce que $q$ est pair. En effet, si on a trouvé d'abord, par la méthode générale, tous les diviseurs quadratiques $py^2+2qyz+rz^2$ de la formule $t^2+au^2$, il ne restera à transformer que ceux dans lesquels $q$ seroit impair; et comme alors l'un des nombres $p$ et $r$ doit être pair et l'autre impair, si on prend $p$ pour celui-ci, il suffira de mettre $y-z$ à la place de $y$, et le coefficient moyen $2q$ deviendra $2q-2p$, c'est-à-dire sera de la forme requise $4\varphi$.

Maintenant, puisque tous les diviseurs quadratiques sont réduits à la forme $py^2+4\varphi yz+\pi z^2$, et qu'on a $p\pi=4\varphi^2+a$, il s'ensuit que $p\pi$ est de la forme $4n-1$, et qu'ainsi les deux coefficiens $p$ et $\pi$ sont, l'un de la forme $4n+1$, l'autre de la forme $4n-1$. On voit par-là que chaque forme quadratique $py^2+4\varphi yz+\pi z^2$ contient à-la-fois des diviseurs $4n+1$ et des diviseurs $4n-1$; mais il est facile de séparer ces deux formes l'une de l'autre, comme cela a lieu dans les Tables III et IV. En effet, si $p$ est de la forme $4n+1$, et qu'on fasse $z=2u$, il est clair que la formule $py^2+8\varphi yu+4\pi u^2$ ne représentera que des diviseurs $4n+1$; au contraire, si l'on fait $y=2u$, la formule $4pu^2+8\varphi zu+\pi z^2$ ne représentera que des diviseurs $4n-1$.

(221) Quant aux formes linéaires qui répondent aux diviseurs quadratiques, elles peuvent de même se partager en deux sortes, les unes $4n+1$, les autres $4n-1$; c'est ce qu'il suffira de développer dans un exemple.

On

On voit dans la Table, que la formule $t^2+11u^2$ n'a que le seul diviseur quadratique à coefficiens impairs $y^2+yz+3z^2$. Ce diviseur en renferme deux autres de forme ordinaire, savoir :

$$y^2+11z^2$$
$$3y^2+2yz+4z^2.$$

De ces deux diviseurs qu'on auroit trouvés immédiatement par la méthode générale, l'un a le coefficient moyen zéro, et partant de la forme $4\nu$; pour réduire l'autre à la même forme, il faut mettre $y-z$ à la place de $z$, ce qui donnera pour transformée $3y^2+4yz+5z^2$. De-là résultent deux diviseurs quadratiques $4n+1$, savoir :

$$y^2+44z^2$$
$$5y^2+8yz+12z^2,$$

et deux diviseurs quadratiques $4n-1$, savoir :

$$11y^2+4z^2$$
$$3y^2+8yz+20z^2.$$

Quant aux formes linéaires correspondantes, on les déduira facilement de celles qui sont données dans la Table, savoir, $22x+1$, 3, 5, 9, 15. Ainsi, pour avoir les formes $4n+1$, on conservera les nombres déterminés 1, 5, 9 qui sont de cette forme, et aux deux autres 3, 15 on ajoutera 22, ce qui fera en tout les cinq formes $44x+1$, 5, 9, 25, 37 : on trouvera semblablement les formes $4n-1$ qui seront $44x+3$, 15, 23, 27, 31. Donc si l'on veut séparer dans la Table les formes $4n+1$ des formes $4n-1$, il faudra substituer l'article suivant à celui qu'on voit dans la Table concernant les diviseurs de $t^2+11u^2$.

| *Diviseurs quadratiques.* | *Diviseurs linéaires.* |
|---|---|
| $y^2+44z^2$<br>$5y^2+8yz+12z^2$ | $44x+1$, 5, 9, 25, 37 |
| $11y^2+4z^2$<br>$3y^2+8yz+20z^2$ | $44x+3$, 15, 23, 27, 31. |

Il n'est pas nécessaire de faire observer que l'article tel qu'il est inséré dans la Table, est beaucoup plus court sans être moins général. Mais il est bon, ponr l'objet d'une démonstration subséquente, de s'être assuré en général de la possibilité de séparer

les diviseurs $4n+1$ des diviseurs $4n-1$, tant dans leurs formes linéaires que dans leurs formes quadratiques.

(222) Enfin, ponr ne rien omettre de ce qui peut abréger la recherche des diviseurs quadratiques, nous ajouterons encore deux mots sur le cas de $a=8n+7$. Si donc on a $a=8n+7$, et qu'on suppose $q$ impair dans le divisenr quadratique $py^2+2qyz+rz^2$, ce diviseur prendra la forme $py^2+2qyz+8mz^2$, où l'on aura $pm=\frac{q^2+a}{8}$. Dans cette forme, on peut snpposer $q$ plus petit qne $4m$, et non plus grand que $r$; par conséquent $q$ sera moindre que $\sqrt{a}$. On essaiera donc pour $q$ tous les nombres impairs 1, 3, 5... jusqu'à $\sqrt{a}$; on calculera pour chaque valeur de $q$ celle de $pm=\frac{q^2+a}{8}$, et on verra si cette valenr peut se décomposer en deux facteurs, l'un $p$ impair et non moindre que $q$, l'autre $m$ pair ou impair, mais $>\frac{q}{4}$. Autant de fois cette condition pourra être remplie, autant on aura de diviseurs quadratiques de la formule $t^2+au^2$, diviseurs qui pourront ensuite être réduits soit à la forme ordinaire où $2q$ est $<p$ et $r$, soit même à la forme dont nous avons fait mention où $q$ est pair. Cette méthode est très-prompte, puisqu'elle n'opère que sur des nombres $pm$ toujours moindres que $\frac{a}{4}$, tandis que dans la méthode générale $pr$ peut aller jusqu'à $\frac{4a}{3}$.

## TABLE VI.

(223) La Table VI contient les diviseurs tant quadratiques que linéaires de la formule $t^2+2au^2$, $a$ étant un nombre de la forme $4n+1$, qui n'est ni quarré, ni divisible par un quarré.

Les diviseurs quadratiques sont réduits à la forme $py^2+4\varphi yz+2mz^2$, où l'on a $pm=2\varphi^2+a$. Or il est aisé de voir que sans changer cette forme, on peut supposer $2\varphi$ moindre ou non plus grand qne $p$ et $m$, ce qui donnera $pm>4\varphi^2$ et $\varphi<\sqrt{\frac{1}{2}a}$; donc si d'après ces conditions on satisfait de toutes les manières possibles à l'équa-

tion $pm=2\varphi^2+a$, on en déduira immédiatement tous les diviseurs quadratiques de la formule $t^2+2au^2$, réduits à la forme $py^2+4\varphi yz+2mz^2$. Ce procédé est beaucoup plus court que la méthode générale, puisque $\sqrt{\frac{1}{2}a}$ est plus petit que $\sqrt{\frac{8}{3}a}$.

Chaque forme $py^2+4\varphi yz+2mz^2$ et sa conjuguée $2py^2+4\varphi yz+mz^2$ résultent à-la-fois d'une même valeur de $pm$ qui satisfait aux conditions requises.

Si le nombre $p$ est de la forme $8n+1$ ou $8n+3$, le diviseur quadratique $py^2+4\varphi yz+2mz^2$ ne comprendra que des nombres de ces mêmes formes $8n+1$ ou $8n+3$; car comme $y$ est toujours impair, si $z$ est pair, le diviseur dont il s'agit sera toujours de la forme $p+8k$, c'est-à-dire de la même forme que $p$. Si $z$ est impair, le diviseur quadratique deviendra, en omettant les multiples de 8, $p+4\varphi+2m$. Soit d'abord $p=8n+1$, à cause de $pm=2\varphi^2+a$, on aura (toujours en omettant les multiples de 8) $m=2\varphi^2+a$, et par conséquent $p+4\varphi+2m=1+4\varphi+4\varphi^2+2a=1+2a=3$; donc le diviseur quadratique deviendra de la forme $8n+3$. Soit en second lieu $p=8n+3$, on aura $3m=2\varphi^2+a$, $6m=4\varphi^2+2a$, et $p+4\varphi+2m=3+4\varphi-4\varphi^2-2a=3-2a=1$; donc le diviseur est de la forme $8n+1$.

On démontrera de même que si $p$ est de l'une des formes $8n+5$, $8n+7$, le diviseur quadratique $py^2+4\varphi yz+2mz^2$ ne contiendra que des nombres de ces mêmes formes $8n+5$, $8n+7$.

Donc tous les diviseurs quadratiques de la formule $t^2+2au^2$, $a$ étant de la forme $4n+1$, se divisent en deux espèces, l'une contenant tous les diviseurs $8n+1$, $8n+3$, l'autre contenant tous les diviseurs $8n+5$, $8n+7$.

(224) Chaque diviseur quadratique, tel qu'il est inséré dans la Table, contient deux formes à-la-fois; mais elles peuvent être facilement séparées, ainsi qu'il résulte de la démonstration précédente.

Soit la formule proposée $t^2+42u^2$, et considérons d'abord le diviseur quadratique $y^2+42z^2$, auquel répondent les formes linéaires $168x+1, 25, 43, 67, 121, 163$. Ce diviseur quadratique appartient, comme on voit, aux formes $8n+1$, $8n+3$; pour les séparer l'une

de l'autre, j'observe que si $z$ est pair, ou si à la place de $z$ on met $2z$, le diviseur deviendra $y^2+168z^2$, et ne contiendra plus que les formes $8n+1$. Si au contraire on suppose $y$ et $z$ impairs à-la-fois; ou si, pour exprimer cette condition, on met $2y+z$ à la place de $y$, le diviseur deviendra $4y^2+4yz+43z^2$, et ne contiendra plus que des formes $8n+3$. Traitant donc semblablement les trois diviseurs quadratiques de la formule proposée $t^2+42u^2$, on aura les résultats suivans :

*Diviseurs* $8n+1$.

| *Quadratiques.* | *Linéaires.* |
|---|---|
| $y^2+168z^2$ | $168x+1,\ 25,\ 121$ |
| $17y^2+12yz+12z^2$ | $168x+17,\ 41,\ 89$ |

*Diviseurs* $8n+3$.

| | |
|---|---|
| $43y^2+4\ \ z+4z^2$ | $168x+43,\ 67,\ 163$ |
| $3y^2+56z^2$ | $168x+59,\ 83,\ 131$ |

*Diviseurs* $8n+5$.

| | |
|---|---|
| $21y^2+8z^2$ | $168x+29,\ 53,\ 149$ |
| $13y^2+24yz+24z^2$ | $168x+13,\ 61,\ 157$ |

*Diviseurs* $8n+7$.

| | |
|---|---|
| $7y^2+24z^2$ | $168x+31,\ 55,\ 103$ |
| $23y^2+8yz+8z^2$ | $168x+23,\ 71,\ 95$ |

Les diviseurs linéaires sont, comme on voit, divisés en huit groupes de trois termes chacun, ce qui est conforme à la loi générale (n°. 203).

## TABLE VII.

(225) La Table VII contient les diviseurs linéaires et quadratiques de la formule $t^2+2au^2$, dans laquelle $a$ est un nombre de la forme $4n-1$, non divisible par un quarré.

Les diviseurs quadratiques sont réduits comme dans la Table précédente à la forme $py^2 + 4\varphi yz + 2mz^2$, dans laquelle on a $mp = 2\varphi^2 + a$; de sorte que la détermination de ces formes se fait toujours de la même manière.

Si le coefficient $p$ est de la forme $8n+3$ ou $8n+5$, le diviseur quadratique $py^2+4\varphi yz+2mz^2$ ne comprendra que des nombres $8n+3$ ou $8n+5$; si le coefficient $p$ est de la forme $8n+1$ ou $8n+7$, le diviseur ne comprendra qne des nombres de ces mêmes formes $8n+1$ et $8n+7$. C'est ce que l'on démontrera comme nons l'avons fait dans l'explication de la Table précédente.

Il s'ensuit par conséquent que tous les divisenrs quadratiques de la formule $t^2+2au^2$, $a$ étant un nombre de la forme $4n-1$, se divisent en deux espèces, l'nne contenant tous les nombres $8n+3$, $8n+5$; l'autre contenant tous les nombres $8n+1$, $8n+7$. Et indépendamment de ces nombres impairs, il est clair que chaque diviseur quadratique $py^2+4\varphi yz+2mz^2$ contient aussi des nombres pairs, puisqu'on peut prendre $y$ pair et $z$ impair, pourvu qu'ils soient premiers entr'enx.

On pourra de même séparer les diviseurs tant quadratiques que linéaires, en quatre espèces qui répondent anx quatre formes $8n+1$, $8n+3$, $8n+5$, $8n+7$.

---

## §. XII. *Suite de Théorêmes contenus dans les Tables précitées.*

(226) Théorème général. *Soit* $4cx+a$ *l'une des formes linéaires qui conviennent aux diviseurs de* $t^2 \pm cu^2$, *je dis que tout nombre premier compris dans la forme* $4cx+a$ *sera nécessairement diviseur de la formule* $t^2 \pm cu^2$, *et sera par conséquent de l'une des formes quadratiques* $py^2+2qyz \pm rz^2$ *qui répondent à la forme linéaire* $4cx+a$.

Ainsi en prenant dans la Table VII l'exemple de la formule $t^2+30u^2$, et choisissant dans cet exemple les formes linéaires qui répondent au diviseur quadratique $15y^2+2z^2$, on peut affirmer que tout nombre premier de l'une des formes $120x+17, 23, 47, 113$ est diviseur de $t^2+30u^2$, et conséquemment doit être de la forme $15y^2+2z^2$.

Par un autre exemple pris dans la même Table, on peut affirmer que tout nombre premier de l'une des formes $56x+3, 5, 13, 19, 27, 45$ est diviseur de $t^2+14u^2$, et par conséquent doit être de la forme $3y^2+4yz+6z^2$.

La démonstration de ce théorême a été donnée ci-dessus, lorsque $c$ est un nombre premier ou le double d'un nombre premier; elle peut être aussi établie sans difficulté pour toute valeur de $c$, si le nombre premier $A$ de la forme $4cx+a$, est en même temps de la forme $4n-1$, car alors il est nécessaire que le nombre $A$ divise la formule $t^2+cu^2$ ou la formule $t^2-cu^2$ (n°. 172). Or si on cherche les formes linéaires des diviseurs de $t^2-cu^2$, ces formes seront trouvées différentes de celles des diviseurs de $t^2+cu^2$; donc le nombre $A$, s'il est de l'une de ces dernières formes, ne peut diviser $t^2-cu^2$; donc il divisera nécessairement $t^2+cu^2$, et sera par conséquent de l'une des formes quadratiques qui répondent à ces formes linéaires.

Le même raisonnement n'auroit plus lieu si $A$ étoit de la forme $4n+1$; il est même incomplet dans le cas de $A=4n-1$, parce

qu'il suppose le développement effectif des diviseurs linéaires tant de la formule $t^2+cu^2$ que de la formule $t^2-cu^2$, c'est pourquoi il convient de suivre une autre route pour parvenir à la démonstration générale de la proposition.

(227) Observons d'abord que la forme linéaire $4cx+a$, à laquelle se rapporte le nombre premier $A$, peut toujours être censée l'une de celles qui répondent à un diviseur quadratique. Soit ce diviseur $py^2+2qyz\pm rz^2$, et on pourra supposer $py^2+2qyz\pm rz^2=4cx+a$; ou, ce qui est la même chose,

$$py^2+2qyz\pm rz^2=4cx+A.$$

Cette équation multipliée par $p$, donnera

$$(py+qz)^2\pm cz^2=4pcx+Ap,$$

d'où l'on voit que $\frac{(py+qz)^2-Ap}{c}$ est un entier; donc, à plus forte raison, si $\theta$ est un nombre premier qui divise $c$, l'équation $\frac{x^2-pA}{\theta}=e$ sera résoluble, et par conséquent on aura $\left(\frac{pA}{\theta}\right)=1$, ou $\left(\frac{p}{\theta}\right)\cdot\left(\frac{A}{\theta}\right)=1$, mais en général on a $\left(\frac{p}{\theta}\right)=+1$ ou $-1$, donc $\left(\frac{p}{\theta}\right)\cdot\left(\frac{p}{\theta}\right)=1$, et par conséquent $\left(\frac{A}{\theta}\right)=\left(\frac{p}{\theta}\right)$.

Nous pourrions considérer le cas particulier de $p=1$, et celui de $p=$ à un quarré, dans lesquels on conclut aisément que $A$ doit être un diviseur de la formule proposée $t^2\pm cu^2$ (1); mais il vaut mieux suivre la démonstration dans toute sa généralité.

(228) Nous avons vu ci-dessus que les diviseurs $4n+1$ et $4n-1$ sont distingués par des formes quadratiques particulières, et même lorsque la formule proposée est $t^2+2au^2$, les diviseurs se subdivisent en quatre formes $8n+1$, $8n+3$, $8n+5$, $8n+7$, et ceux-ci sont contenus chacun dans des formes quadratiques distinctes. On pourra donc supposer que le diviseur quadratique $py^2+2qyz\pm 2mz^2$ qui répond à la forme linéaire $4cx+a$ ou $4cx+A$ ne contient que des nombres de la même espèce que $A$, c'est-à-dire tels que la

(1) Le double signe indique seulement que la formule proposée peut être $t^2+cu^2$ ou $t^2-cu^2$; mais d'ailleurs il ne laisse aucune indétermination.

différence de ces nombres avec $A$ est divisible par 4 et même par 8, si la formule est $t^2+2au^2$, ou si l'on a $2pm-q^2=2a$. Par conséquent $p$ qui est l'un de ces nombres, sera tel que $\frac{p-A}{4}$ est un entier, ou même que $\frac{p-A}{8}$ en est un, si $c=2a$.

Nous supposerons de plus que le coefficient $p$ est un nombre premier; s'il ne l'étoit pas, on chercheroit un nombre premier compris dans la formule $py^2+2qyz\pm 2mz^2$. Soit ce nombre $p'=p\mu^2+2q\mu\nu\pm 2m\nu^2$, si l'on détermine $\mu^\circ$ et $\nu^\circ$ d'après l'équation $\mu\nu^\circ-\mu^\circ\nu=1$, et qu'on fasse $y=\mu y'+\mu^\circ z'$, $z=\nu y'+\nu^\circ z'$, on aura pour transformée le diviseur quadratique $p'y'y'+2q'y'z'\pm 2m'z'z'$, dans lequel le coefficient du premier terme est un nombre premier. Ainsi, en regardant cette préparation comme déjà faite, il est permis de supposer $p$ un nombre premier.

Reprenons maintenant l'équation déjà trouvée $\left(\frac{A}{\theta}\right)=\left(\frac{p}{\theta}\right)$, où $\theta$ désigne un diviseur premier quelconque de $c$; soient $\alpha, \alpha', \alpha''$, &c. les diviseurs premiers $4n+1$, et $\zeta, \zeta', \zeta''$... les diviseurs premiers $4n-1$, nous aurons, en mettant ces nombres au lieu de $\theta$,

$$\left(\frac{A}{\alpha}\right)=\left(\frac{p}{\alpha}\right),\quad \left(\frac{A}{\alpha'}\right)=\left(\frac{p}{\alpha'}\right),\quad \left(\frac{A}{\alpha''}\right)=\left(\frac{p}{\alpha''}\right),\ \text{\&c.}$$

$$\left(\frac{A}{\zeta}\right)=\left(\frac{p}{\zeta}\right),\quad \left(\frac{A}{\zeta'}\right)=\left(\frac{p}{\zeta'}\right),\quad \left(\frac{A}{\zeta''}\right)=\left(\frac{p}{\zeta''}\right),\ \text{\&c.}$$

De-là on déduit par la loi de réciprocité, et parce que $A$ et $p$ sont tous deux de la forme $4n+1$, ou tous deux de la forme $4n-1$,

$$\left(\frac{\alpha}{A}\right)=\left(\frac{\alpha}{p}\right),\quad \left(\frac{\alpha'}{A}\right)=\left(\frac{\alpha'}{p}\right),\quad \left(\frac{\alpha''}{A}\right)=\left(\frac{\alpha''}{p}\right),\ \text{\&c.}$$

$$\left(\frac{\zeta}{A}\right)=\left(\frac{\zeta}{p}\right),\quad \left(\frac{\zeta'}{A}\right)=\left(\frac{\zeta'}{p}\right),\quad \left(\frac{\zeta''}{A}\right)=\left(\frac{\zeta''}{p}\right),\ \text{\&c.}$$

Donc 1°. si $c$ est impair, il sera égal au produit de tous les nombres premiers $\alpha, \alpha', \alpha''$.... $\zeta, \zeta', \zeta''$,... et on aura

$$\left(\frac{c}{A}\right)=\left(\frac{\alpha}{A}\right)\cdot\left(\frac{\alpha'}{A}\right)\cdot\left(\frac{\alpha''}{A}\right)\cdots\left(\frac{\zeta}{A}\right)\cdot\left(\frac{\zeta'}{A}\right)\cdot\left(\frac{\zeta''}{A}\right)\cdots$$

$$\left(\frac{c}{p}\right)=\left(\frac{\alpha}{p}\right)\cdot\left(\frac{\alpha'}{p}\right)\cdot\left(\frac{\alpha''}{p}\right)\cdots\left(\frac{\zeta}{p}\right)\cdot\left(\frac{\zeta'}{p}\right)\cdot\left(\frac{\zeta''}{p}\right)\cdots,$$

Et

Et puisque les facteurs de ces expressions sont égaux chacun à chacun, on aura $\left(\frac{c}{A}\right)=\left(\frac{c}{p}\right)$.

2°. Si $c$ est pair, outre les facteurs précédens, $c$ contiendra le facteur 2; mais puisque $p$ et $A$ sont de même forme par rapport aux multiples de 8, on a $\left(\frac{2}{A}\right)=\left(\frac{2}{p}\right)$, donc on aura encore $\left(\frac{c}{A}\right)=\left(\frac{c}{p}\right)$.

Mais $p$ étant diviseur de $q^2 \pm c$, on a $\left(\frac{\mp c}{p}\right)=1$; donc on a aussi $\left(\frac{\mp c}{A}\right)=1$; donc le nombre premier $A$ est toujours diviseur de la formule proposée $t^2 \pm cu^2$. Donc il doit être de l'une des formes quadratiques qui répondent à la forme linéaire $4cx+a$.

(229) La proposition que nous venons de démontrer, est sans contredit l'une des plus générales et des plus importantes de la théorie des nombres; la démonstration que nous en avons donnée suppose seulement qu'il existe un nombre premier compris dans le diviseur quadratique $py^2+2qyz+rz^2$. Or cette supposition n'a rien que de très-admissible, et elle se vérifie aisément à l'égard de toutes les formes quadratiques renfermées dans nos tables; il n'y a même aucun doute que la formule $py^2+2qyz+rz^2$ ne contienne une infinité de nombres premiers, excepté seulement dans le cas où les trois nombres $p$, $q$, $r$ auroient un commun diviseur $\theta$; mais ils ne peuvent en avoir, puisque $c$ ou $pr-q^2$ est supposé n'avoir aucun facteur quarré.

On pourroit néanmoins rendre la démonstration tout-à-fait indépendante de la supposition que $p$ est un nombre premier; il faudroit pour cela examiner différens cas, selon le nombre des facteurs dont $c$ est composé.

On a déjà examiné les cas où $c$ est un nombre premier ou le double d'un tel nombre : supposons donc maintenant $c=\alpha\mathcal{C}$, $\alpha$ et $\mathcal{C}$ étant deux nombres premiers impairs à volonté; soit en même temps $py^2+2qyz+2mz^2$ la forme quadratique qui répond à la

Nn

forme linéaire $4cx+a$ ou $4cx+A$, de sorte que $p$ et $A$ seront tous deux de l'espèce $4n+1$, ou tous deux de l'espèce $4n-1$. On aura donc par hypothèse

$$py^2+2qyz+2mz^2=4cx+A$$

et en multipliant par $p$,

$$(py+qz)^2+cz^2=4cpx+Ap.$$

( On ne considère ici que le cas de $c$ positif, celui de $c$ négatif pouvant être traité d'une manière semblable. )

Maintenant puisque $c=\alpha\beta$, on aura successivement, par rapport à $\alpha$ et $\beta$, les équations $\left(\frac{Ap}{\alpha}\right)=1$, $\left(\frac{Ap}{\beta}\right)=1$, lesquelles donnent

$$\left(\frac{A}{\alpha}\right)=\left(\frac{p}{\alpha}\right), \quad \left(\frac{A}{\beta}\right)=\left(\frac{p}{\beta}\right).$$

Soit $p=\pi\pi'\pi''\pi'''$ &c., $\pi$, $\pi''$, $\pi^{IV}$, &c. étant des nombres premiers $4n+1$, et $\pi'$, $\pi'''$, &c. des nombres premiers $4n-1$; si $p$ étoit divisible par des quarrés, on les omettroit entièrement, pour ne conserver que les facteurs inégaux. On aura donc

$$\left(\frac{A}{\alpha}\right)=\left(\frac{\pi}{\alpha}\right)\cdot\left(\frac{\pi'}{\alpha}\right)\cdot\left(\frac{\pi''}{\alpha}\right)\cdot \text{ \&c.}$$

$$\left(\frac{A}{\beta}\right)=\left(\frac{\pi}{\beta}\right)\cdot\left(\frac{\pi'}{\beta}\right)\cdot\left(\frac{\pi''}{\beta}\right)\cdot \text{ \&c.}$$

Mais l'équation $2pm-q^2=c=\alpha\beta$, donne

$$\left(\frac{-\alpha\beta}{\pi}\right)=1, \quad \left(\frac{-\alpha\beta}{\pi'}\right)=1, \quad \left(\frac{-\alpha\beta}{\pi''}\right)=1, \text{ \&c.}$$

et ainsi par rapport à tout facteur de $p$. On aura donc

$$\left(\frac{\alpha}{\pi}\right)=\left(\frac{\beta}{\pi}\right), \quad \left(\frac{\alpha}{\pi''}\right)=\left(\frac{\beta}{\pi''}\right), \quad \left(\frac{\alpha}{\pi^{IV}}\right)=\left(\frac{\beta}{\pi^{IV}}\right), \text{ \&c.}$$

$$\left(\frac{\alpha}{\pi'}\right)=-\left(\frac{\beta}{\pi'}\right), \quad \left(\frac{\alpha}{\pi'''}\right)=-\left(\frac{\beta}{\pi'''}\right), \text{ \&c.}$$

De-là on déduit par la loi de réciprocité (n°. 164)

$$\left(\frac{\pi}{\alpha}\right)=\left(\frac{\pi}{\beta}\right), \left(\frac{\pi''}{\alpha}\right)=\left(\frac{\pi''}{\beta}\right), \left(\frac{\pi^{IV}}{\alpha}\right)=\left(\frac{\pi^{IV}}{\beta}\right), \text{ \&c.}$$

$$\left(\frac{\pi'}{\alpha}\right)=(-1)^{\frac{\alpha+\beta}{2}}\left(\frac{\pi'}{\beta}\right), \left(\frac{\pi'''}{\alpha}\right)=(-1)^{\frac{\alpha+\beta}{2}}\left(\frac{\pi'''}{\beta}\right), \text{ \&c.}$$

Ces dernières seulement ont besoin de quelqu'explication : or la loi générale donne $\left(\frac{\pi'}{\alpha}\right)=(-1)^{\frac{\pi'-1}{2}\cdot\frac{\alpha-1}{2}}\cdot\left(\frac{\alpha}{\pi'}\right)$ ; et parce que $\frac{\pi'-1}{2}$ est impair, cette équation devient $\left(\frac{\pi'}{\alpha}\right)=(-1)^{\frac{\alpha+1}{2}}\left(\frac{\alpha}{\pi'}\right)$ : on aura de même $\left(\frac{\pi'}{\beta}\right)=(-1)^{\frac{\beta-1}{2}}\left(\frac{\beta}{\pi'}\right)$ ; donc puisque $\left(\frac{\alpha}{\pi'}\right)=-\left(\frac{\beta}{\pi'}\right)$, il en résulte $\left(\frac{\pi'}{\alpha}\right)=(-1)^{\frac{\alpha+\beta}{2}}\left(\frac{\pi'}{\beta}\right)$, et ainsi des autres relatives à $\pi'''$, $\pi^{v}$, &c.

Multipliant entr'elles les deux suites d'équations qui précèdent, on aura $\left(\frac{p}{\alpha}\right)=(-1)^{\frac{\alpha+\beta}{2}\cdot k}\left(\frac{p}{\beta}\right)$, $k$ étant le nombre des facteurs $\pi'$, $\pi'''$, &c. de la forme $4n-1$.

Soit d'abord $\mathcal{A}$, et par conséquent $p$ de la forme $4n+1$, il faudra que le nombre $k$ soit pair, et ainsi on aura $\left(\frac{p}{\alpha}\right)=\left(\frac{p}{\beta}\right)$ ; donc aussi $\left(\frac{\mathcal{A}}{\alpha}\right)=\left(\frac{\mathcal{A}}{\beta}\right)$ ; il s'ensuit réciproquement $\left(\frac{\alpha}{\mathcal{A}}\right)=\left(\frac{\beta}{\mathcal{A}}\right)$, ou $\left(\frac{\alpha\beta}{\mathcal{A}}\right)=1$, donc $\mathcal{A}$ est diviseur $t^2+\alpha\beta u^2$.

Soient en second lieu $\mathcal{A}$ et $p$ de la forme $4n-1$, le nombre $k$ sera impair, et on aura $\left(\frac{p}{\alpha}\right)=(-1)^{\frac{\alpha+\beta}{2}}\left(\frac{p}{\beta}\right)$ ; donc $\left(\frac{\mathcal{A}}{\alpha}\right)=(-1)^{\frac{\alpha+\beta}{2}}\left(\frac{\mathcal{A}}{\beta}\right)$. De-là on déduit par la loi de réciprocité

$$(-1)^{\frac{\alpha-1}{2}}\left(\frac{\alpha}{\mathcal{A}}\right)=(-1)^{\frac{\alpha+\beta}{2}+\frac{\beta-1}{2}}\left(\frac{\beta}{\mathcal{A}}\right);$$

ce qui se réduit à $\left(\frac{\alpha}{\mathcal{A}}\right)=(-1)^{\beta}\left(\frac{\beta}{\mathcal{A}}\right)$, ou $\left(\frac{\alpha}{\mathcal{A}}\right)=-\left(\frac{\beta}{\mathcal{A}}\right)$. Donc $\left(\frac{-\alpha\beta}{\mathcal{A}}\right)=1$ ; donc $\mathcal{A}$ est encore diviseur de $t^2+\alpha\beta u^2$.

La conclusion que $\mathcal{A}$ est diviseur de $t^2+cu^2$ a donc lieu, quel que soit le coefficient $p$, et il n'y a pas de doute qu'elle ne se vérifiât égalemeut, si $c$ étoit le produit de plus de deux nombres premiers.

(230) On voit maintenant que chaque article de nos Tables fournit plusieurs théorêmes qui donnent des rapports entre les formes linéaires des nombres premiers et leurs formes quadratiques. Voici les plus mémorables de ces théorêmes, ou ceux qui s'appliquent aux formules les plus simples.

*D'après la Table III.*

1. Tout nombre premier $8x+1$ ou $8x+7$ est de la forme $y^2-2z^2$.
2. Tout nombre premier $12x+1$ est de la forme $y^2-3z^2$.
   Et tout nombre premier $12x+11$ est de la forme $3y^2-z^2$.
3. Tout nombre premier de l'une des formes $20x+1$, $20x+9$, $20x+11$, $20x+19$, est de la forme $y^2-5z^2$.
4. Tout nombre premier $24x+1$ ou $24x+19$ est de la forme $y^2-6z^2$, et tout nombre premier $24x+5$ ou $24x+23$ est de la forme $6y^2-z^2$.
5. Tout nombre premier $28x+1$, 9, 25 est de la forme $y^2-7z^2$, et tout nombre premier $28x+3$, $28x+19$, $28x+27$ est de la forme $7y^2-z^2$.
6. Tout nombre premier $40x+1, 9, 31, 39$ est de la forme $y^2-10z^2$, et tout nombre premier $40x+3$, 13, 27, 37 est de la forme $2y^2-5z^2$.
7. &c.

*D'après la Table IV.*

1. Tout nombre premier $4x+1$ est de la forme $y^2+z^2$.
2. Tout nombre premier $20x+1$ ou $20x+9$ est de la forme $y^2+5z^2$, et tout nombre premier $20x+3$ ou $20x+7$, est de la forme $2y^2+2yz+3z^2$.
3. Tout nombre premier $52x+1$, 9, 17, 25, 29, 49 est de la forme $y^2+13z^2$, et tout nombre premier $52x+7$, 11, 15, 19, 31, 47, est de la forme $2y^2+2yz+7z^2$.
4. &c.

*D'après la Table V.*

1. Tout nombre premier $6x+1$ est de la forme $y^2+yz+z^2$, ou, ce qui revient au même, de la forme $y^2+3z^2$.

2. Tout nombre premier $14x+1$, $9$, $11$ est de la forme $y^2+7z^2$.

3. Tout nombre premier $22x+1$, $3$, $5$, $9$, $15$, est de la forme $y^2+yz+3z^2$.

4. Tout nombre premier $30x+1$ ou $30x+19$ est de la forme $y^2+15z^2$, et tout nombre premier $30x+17$ ou $30x+23$ est de la forme $3y^2+5z^2$.

5. &c.

*D'après la Table VI.*

1. Tout nombre premier $8x+1$ ou $8x+3$ est de la forme $y^2+2z^2$.

2. Tout nombre premier $40x+1, 9, 11, 19$ est de la forme $y^2+10z^2$, et tout nombre premier $40x+7$, $13$, $23$, $37$ est de la forme $2y^2+5z^2$.

3. Tout nombre premier $104x+1$, $3$, $9$, $17$, $25$, $27$, $35$, $43$, $49$, $51$, $75$, $81$, est de l'une des formes $y^2+26z^2$, $3y^2+4yz+10z^2$; et tout nombre premier $104x+5$, $7$, $15$, $21$, $31$, $37$, $45$, $47$, $63$, $71$, $85$, $93$, est de l'une des formes $2y^2+13z^2$, $6y^2+4yz+5z^2$.

4. &c.

*D'après la Table VII.*

1. Tout nombre premier $24x+5$ ou $24x+11$ est de la forme $2y^2+3z^2$, et tout nombre premier $24x+1$ ou $24x+7$ est de la forme $y^2+6z^2$.

2. Tout nombre premier $56x+3$, $5$, $13$, $19$, $27$, $45$ est de la forme $3y^2+4yz+6z^2$, et tout nombre premier $56x+1$, $9$, $15$, $23$, $25$, $39$ est de l'une des formes $y^2+14z^2$, $2y^2+7z^2$.

3. Tout nombre premier $88x+13$, $19$, $21$, $29$, $35$, $43$, $51$, $61$, $83$, $85$ est de la forme $2y^2+11z^2$, et tout nombre premier $88x+1$, $9$, $15$, $23$, $25$, $31$, $47$, $49$, $71$, $81$ est de la forme $y^2+22z^2$.

4. Tout nombre premier $120x+11$, $29$, $59$, $101$ est de la forme $5y^2+6z^2$.

Tout nombre premier $120x+13$, $37$, $43$, $67$ est de la forme $10y^2+3z^2$.

Tout nombre premier $120x+1$, 31, 49, 79 est de la forme $y^2+30z^2$.

Tout nombre premier $120x+17$, 23, 47, 113 est de la forme $2y^2+15z^2$.

5. &c., &c.

Lagrange est le premier qui ait ouvert la voie pour la recherche de ces sortes de théorêmes (Voyez Mémoires de Berlin 1775). Mais les méthodes dont ce grand Géomètre s'est servi, ne sont applicables que dans très-peu de cas aux nombres premiers $4n+1$; et la difficulté à cet égard ne pouvoit être résolue complètement qu'à l'aide de la loi de réciprocité qui a été donnée pour la première fois dans les Mémoires de l'Académie des Sciences de Paris, année 1785.

---

## §. XIII. *Autres Théorêmes concernant les formes quadratiques des nombres.*

(231) Soit $P$ un nombre quelconque diviseur de la formule $t^2 \pm cu^2$, et comme tel, renfermé dans le divisenr quadratique $py^2+2qyz \pm rz^2$, on pourra supposer $P = p\alpha^2 + 2q\alpha\beta \pm r\beta^2$. Si ensuite on détermine $\alpha^\circ$ et $\beta^\circ$ d'après l'équation $\alpha\beta^\circ - \alpha^\circ\beta = 1$, et qu'on mette $\alpha y + \alpha^\circ z$ et $\beta y + \beta^\circ z$ à la place de $y$ et $z$, le diviseur quadratique $py^2 + 2qyz \pm rz^2$ deviendra de la forme $Py^2 + 2Qyz + Rz^2$.

Soit $P'$ un autre diviseur contenu dans la même formule $py^2+2qyz \pm rz^2$, ou dans son équivalente $Py^2+2Qyz+Rz^2$, on pourra faire $P' = P\mu^2 + 2Q\mu\nu + R\nu^2$, et ainsi on aura $PP' = (P\mu + Q\nu)^2 \pm c\nu^2$. Donc *si* P *et* P′ *sont deux diviseurs de la formule* $t^2 \pm cu^2$, *tous deux compris dans une même formule quadratique* $py^2+2qyz \pm rz^2$, *leur produit* PP′ *sera toujours de la forme* $t^2 \pm cu^2$.

*Réciproquement si les deux nombres* P *et* P′ *sont tels qu'on ait* $PP' = t^2 \pm cu^2$, t *et* u *étant premiers entr'eux, je dis que ces deux nombres appartiendront à un même diviseur quadratique.*

En effet, puisque $t$ et $u$ sont premiers entr'eux, il faut que $u$ et $P$ le soient aussi; on pourra donc faire $t = Py + Qu$, $y$ et $Q$ étant des indéterminées, ce qui donnera $P' = Py^2 + 2Qyu + \frac{Q^2 \pm c}{P} u^2$. Dans cette expression, $u$ et $P$ n'ayant pas de commun diviseur, on voit que $Q^2 \pm c$ doit être divisible par $P$; ainsi faisant $Q^2 \pm c = PR$, on aura $P' = Py^2 + 2Qyu + Ru^2$. Le second membre, en regardant $y$ et $u$ comme des indéterminées, représente l'un des diviseurs quadratiques de la formule $t^2 \pm cu^2$, et il est évident que ce diviseur contient à-la-fois $P$ et $P'$. Donc *si les deux nombres* P *et* P′, *&c.*

(232) *Tout nombre premier* A *qui divise la formule* $t^2 \pm cu^2$, *ne peut appartenir qu'à un seul diviseur quadratique de cette formule.*

Car si le nombre premier $A$ appartenoit à deux diviseurs quadratiques différens, on pourroit transformer ceux-ci en deux autres, dans lesquels $A$ seroit coefficient du premier terme (n°. 231). Soient ces deux diviseurs

$$Ay^2+2Byz+Cz^2$$
$$Ay^2+2B'yz+C'z^2,$$

on pourra supposer en même temps $A>2B$ et $2B'$; car si on avoit $2B>A$, il faudroit substituer $y-mz$ à la place de $y$, et déterminer $m$ de manière que le coefficient de $yz$ ne fût pas plus grand que $A$. Cela posé, on auroit toujours $B^2-AC = B'^2-AC' = \pm c$; donc $\frac{B^2-B'^2}{A}$ seroit un entier, et puisque $A$ est premier, il faudroit que $A$ divisât l'un des facteurs $B+B'$, $B-B'$. Mais $B$ et $B'$ étant l'un et l'autre plus petits que $\frac{1}{2}A$, les nombres $B+B'$, $B-B'$ seront tous deux plus petits que $A$; donc ils ne seront ni l'un ni l'autre divisibles par $A$, à moins qu'on ne suppose $B'=B$. Mais alors les deux diviseurs quadratiques dont il s'agit, seront identiques; donc le nombre premier $A$ qui divise la formule $t^2\pm cu^2$, ne peut appartenir qu'à un seul diviseur quadratique de cette formule.

*Remarque.* Le même raisonnement auroit lieu, si $A$ étoit le double d'un nombre premier, et en général, si $A$ étoit une puissance quelconque d'un nombre premier, ou le double de cette puissance; car l'équation $\frac{x^2\pm c}{A}=e$ n'admet qu'une seule solution, lorsque $A$ est de la forme mentionnée, ou même plus généralement, lorsque $A=\alpha^n\theta$, ou $2\alpha^n\theta$, $\theta$ étant un diviseur de $c$, et $\alpha$ un nombre premier (Voyez n°. 191). Donc dans tous ces cas, qui sont fort étendus, le nombre $A$ ne pourra être compris que dans un seul diviseur quadratique de la formule $t^2\pm cu^2$.

(233) *Au contraire, si* A *est un nombre composé, il pourra y avoir plusieurs diviseurs quadratiques de la formule* $t^2\pm cu^2$ *qui contiennent le nombre* A.

En effet le diviseur quadratique qui contient $A$ peut se représenter par la formule $Ay^2+2Byz+Cz^2$, où l'on a $2B<A$ et $B^2$

$B^2 - A C = \pm c$. Or $A$ étant connu, on peut prendre pour $B$ tout nombre qui satisfait à l'équation $\frac{x^2 \pm c}{A} = e$, pourvu que cette solution soit comprise entre zéro et $\frac{1}{2} A$. D'ailleurs lorsque $A$ a des facteurs premiers inégaux et non communs avec $c$, on a déjà vu (n°. 191) que cette équation admet un nombre $2^{i-1}$ de solutions, $i$ étant le nombre de ces facteurs (2 excepté). Donc il y aura pareillement un nombre $2^{i-1}$ de diviseurs quadratiques $A y^2 + 2 B y z + C z^2$, ou de formes de diviseurs quadratiques, renfermant $A$. Il pourra arriver cependant que plusieurs de ces diviseurs, réduits à l'expression la plus simple, ne diffèrent point entr'eux; de sorte qu'en vertu de la limite assignée, le nombre des diviseurs quadratiques qui contiennent $A$ ne peut excéder $2^{i-1}$, mais il pourra être plus petit. Cela est d'autant plus manifeste, que le nombre des diviseurs quadratiques d'une même formule $t^2 \pm c u^2$ est souvent très-petit, et se réduit quelquefois à un ou deux, tandis que si l'on prend un nombre $A$ composé de plusieurs facteurs, la quantité $2^{i-1}$ qui représente le nombre des valeurs de $B$ peut devenir aussi grande qu'on voudra.

Jusqu'ici nous avons considéré les diviseurs des deux formules $t^2 + c u^2$, $t^2 - c u^2$ indistinctement; dans le reste de ce paragraphe, nous ne nous occuperons que de la première formule $t^2 + c u^2$, et de ses diviseurs quadratiques.

(234) *Tout nombre premier* A *qui est de la forme* $y^2 + a z^2$, a *étant un nombre positif, ne peut être qu'une seule fois de cette forme, en sorte qu'on ne pourroit avoir à-la-fois* $A = f^2 + a g^2$ *et* $A = f'^2 + a g'^2$, $g'$ *étant différent de* g.

Supposons, s'il est possible, que ces deux formes aient lieu à-la-fois, et qu'en conséquence on ait $f^2 + a g^2 = f'^2 + a g'^2$, ou $f^2 - f'^2 = a(g'^2 - g^2)$, il faudra que $f + f'$ soit divisible par un facteur de $a$ et $f - f'$ par l'autre facteur. Soit donc $a = mn$, $m$ et $n$ étant deux facteurs indéterminés; et on aura $f + f' = m h$, $f - f' = n k$, ce qui donnera $h k = g'^2 - g^2$. Soit $\varphi$ le plus grand commun diviseur de $h$ et de $g' + g$, on pourra faire $h = \mu \varphi$, $g + g' = \nu \varphi$, et il restera à satisfaire à l'équation $\mu k = (g' - g) \nu$. Or puisque $\mu$ et $\nu$ sont pre-

miers entr'eux, il faudra qu'on ait $k=\nu\psi$, $g'-g=\mu\psi$, $\psi$ étant une nouvelle indéterminée. De là résulte

$$f=\tfrac{1}{2}(mh+nk)=\tfrac{1}{2}(m\mu\varphi+n\nu\psi)$$
$$g=\tfrac{1}{2}(\nu\varphi-\mu\psi).$$

Donc $f^2+ag^2$ ou $A=\frac{1}{4}(m\mu^2+n\nu^2)\,(m\varphi^2+n\psi^2)$. Et puisque $A$ est un nombre premier, il faudra que l'un des facteurs du second membre, par exemple $m\mu^2+n\nu^2$, soit égal à 4 ou à 2.

Soit d'abord $m\mu^2+n\nu^2=2$, on ne peut supposer $\mu=0$ ni $\nu=0$, parce que l'une ou l'autre supposition rendroit identiques les deux formes $f^2+ag^2$, $f'^2+ag'^2$; donc la seule manière de satisfaire à cette équation, est de supposer tous les nombres $m$, $n$, $\mu$, $\nu$ égaux à l'unité. Mais alors on auroit $a=1$, $f=\frac{1}{2}(\varphi+\psi)$, $g=\frac{1}{2}(\varphi-\psi)$, $f'=\frac{1}{2}(\varphi-\psi)$, $g'=\frac{1}{2}(\varphi+\psi)$, donc $f^2+ag^2$ et $f'^2+ag'^2$, ne seroient qu'une seule et même forme $\frac{1}{4}(\varphi+\psi)^2+\frac{1}{4}(\varphi-\psi)^2$, contre la supposition.

En second lieu, soit $m\mu^2+n\nu^2=4$; comme on ne peut faire encore $\mu=0$, ni $\nu=0$, il n'y aura que deux manières de satisfaire à cette équation, l'une en faisant $m=n=2$, $\mu=\nu=1$; l'autre en faisant $m=1$, $n=3$, $\mu=\nu=1$. Le premier cas donneroit $A=2\varphi^2+2\psi^2$, et ainsi $A$ ne seroit pas un nombre premier.

Dans le second cas, on aura $A=\varphi^2+3\psi^2$, $f=\frac{1}{2}(\varphi+3\psi)$, $g=\frac{1}{2}(\varphi-\psi)$; mais ces dernières valeurs ne peuvent avoir lieu, à moins que $\varphi$ et $\psi$ ne soient tous deux pairs ou tous deux impairs, et dans les deux hypothèses $\varphi^2+3\psi^2$ ou $A$ seroit divisible par 4. Donc, dans aucun cas, le nombre premier $A$ ne pourra être exprimé de deux manières différentes par la même formule $y^2+az^2$.

*Remarque.* Si un nombre $A$ peut être exprimé de deux manières par la formule $y^2+az^2$, ce nombre sera nécessairement un nombre composé, et on pourra même, par l'analyse précédente, en déterminer les deux facteurs. Mais il est à observer que ce théorême ne seroit plus vrai si $a$ étoit un nombre négatif, car l'équation $A=y^2-az^2$ étant supposée avoir une solution, elle en a dès-lors une infinité.

(235) Nous avons déjà eu occasion d'observer que le produit des deux formules semblables $x^2+ay^2$, $p^2+aq^2$ donne un produit semblable, lequel est susceptible des deux formes

$$(px-aqy)^2+a(py+qx)^2$$
$$(px+aqy)^2+a(py-qx)^2.$$

C'est ce dont on peut s'assurer par le simple développement de ces quantités. Mais on peut trouver directement la forme de ces produits, en considérant que les deux facteurs $x^2+ay^2$, $p^2+aq^2$ équivalent aux quatre suivans

$$x+y\sqrt{-a},\ x-y\sqrt{-a},\ p+q\sqrt{-a}.\ p-q\sqrt{-a}.$$

Or si on multiplie les deux facteurs $x+y\sqrt{-a}$, $p+q\sqrt{-a}$, l'un par l'autre, le produit sera $px-aqy+(py+qx)\sqrt{-a}$; les deux autres facteurs auront de même pour produit $px-aqy-(py+qx)\sqrt{-a}$; et le produit de ces deux produits sera $(px-aqy)^2+a(py+qx)^2$. Le résultat seroit le même, en changeant le signe de $q$, et ainsi une autre forme du produit est $(px+aqy)^2+a(py-qx)^2$. Ces formules ont lieu, quel que soit le signe de $a$; tout ce qui suit suppose que $a$ est positif.

(236) Si la formule $x^2+ay^2$ représente un nombre composé $N$, lequel soit $m$ fois de la forme $x^2+ay^2$, et que $p^2+aq^2$ représente un nombre premier $A$, on voit, par le n°. précédent, que le produit $NA$ sera susceptible de $2m$ formes semblables à $x^2+ay^2$, pourvu toutefois que $N$ ne soit pas divisible par $A$: on verra tout-à-l'heure pourquoi nous mettons cette restriction.

Si le nombre premier $A$ est de la forme $p^2+aq^2$, le quarré du nombre $A$ sera une fois de la forme $x^2$, et une fois de la forme $x^2+ay^2$; car on a, suivant les formules précédentes,

$$A^2=(p^2+aq^2)^2 \text{ et } A^2=(pp-aqq)^2+a(2pq)^2.$$

Donc si le nombre composé $N$ est $m$ fois de la forme $x^2+ay^2$, et que le nombre premier $A$ soit aussi de la forme $p^2+aq^2$, le produit $NA^2$ sera susceptible de $3m$ formes semblables $X^2+aY^2$; parmi lesquelles il y aura $2m$ formes où $X$ et $Y$ n'auront point de commun diviseur $A$, et $m$ où ils l'auront. On suppose encore que $A$ n'est point diviseur de $N$.

Le nombre premier $A$ étant toujours de la forme $p^2+aq^2$,

le cube de $A$ sera deux fois de cette même forme; car $A^2$ est de la forme $(pp-aqq)^2+a(2pq)^2$; et cette quantité multipliée par $p^2+aq^2$ fournit les deux formes

$$(p^3-3apq^2)^2+a(3p^2q-aq^3)^2$$
$$(p^3+apq^2)^2+a(p^2q+aq^3)^2.$$

La dernière étant représentée par $X^2+aY^2$, on voit que $X$ et $Y$ ont pour commun diviseur $A$, et qu'elle se réduit à $(pA)^2+a(qA)^2$, la même que si on eût multiplié simplement $p^2+aq^2$ par $A^2$.

En général, $A$ étant un nombre premier de la forme $p^2+aq^2$, on peut faire $A^n=P^2+aQ^2$, et on aura, pour déterminer $P$ et $Q$, l'équation $(p+q\sqrt{-a})^n=P+Q\sqrt{-a}$, dans laquelle, après avoir développé le premier membre, il faut égaler la partie rationnelle à la partie rationnelle, et la partie imaginaire à la partie imaginaire.

On aura aussi $A^n=A^2 \cdot A^{n-2}$, de sorte que si on fait $A^{n-2}=P'P'+aQ'Q'$, on aura une nouvelle valeur de $A$ qui sera $(AP')^2+a(AQ')^2$. On en tirera une semblable de $A^4 \cdot A^{n-4}$, &c. Donc autant il y aura d'unités dans $1+\frac{n}{2}$, autant on aura de formes diverses $X^2+aY^2$ pour la puissance $A^n$; mais parmi ces formes, il n'y en aura qu'une seule dans laquelle $X$ et $Y$ seront premiers entr'eux; dans toutes les autres, $X$ et $Y$ auront successivement pour commun diviseur $A$, $A^2$, $A^3$, &c. Donc la valeur de $A^n$ sera

lorsque $n=2$, une fois $A^2$ et une fois de la forme $X^2+aY^2$,
lorsque $n=3$, deux fois de la forme $X^2+aY^2$,
lorsque $n=4$, une fois $A^4$ et deux fois de la forme $X^2+aY^2$,
lorsque $n=5$, trois fois de la forme $X^2+aY^2$,
ainsi de suite.

Et comme chaque facteur $X^2+aY^2$ multiplié par un nombre de même forme, produit deux résultats de cette même forme, tandis que $X^n$ seul n'en donne qu'un, on peut conclure en général que le produit d'une formule $f^2+ag^2$ par $A^n$ sera susceptible de $n+1$ formes semblables $x^2+ay^2$, lesquelles seront toutes différentes entr'elles, pourvu que $A$ ne divise point $f^2+ag^2$.

Donc si on a $N=\alpha^n \beta^{n'} \gamma^{n''}$ &c., $\alpha$, $\beta$, $\gamma$, &c. étant des nombres

premiers, tous de la forme $p^2+aq^2$, le nombre $N$ sera autant de fois de la forme $x^2+ay^2$ qu'il y a d'unités dans le produit

$$\tfrac{1}{2}(n+1)(n'+1)(n''+1)(n'''+1) \&c.$$

Ce nombre coïncide avec la moitié de celui des diviseurs de $N$, ou avec celui qui indique en combien de manières on peut partager $N$ en deux facteurs.

Dans le cas où $(n+1)(n'+1)$ &c. seroit impair, le résultat seroit toujours vrai, pourvu que la fraction restante $\tfrac{1}{2}$ fût comptée pour une unité.

Lorsque $a=1$, ou que la forme dont il s'agit est $x^2+y^2$, le facteur 2 ni ses puissances n'entrent point en considération, et ne changent pas le nombre des formes du produit. Car en multipliant $x^2+y^2$ par 2, on n'a qu'un produit de la même forme, qui est $(x+y)^2+(x-y)^2$.

(237) Pour appliquer la formule générale, considérons les trois nombres 5, 13, 17, qui tous sont de la forme $p^2+q^2$, on trouvera :

1°. Que le produit 5.13.17 sera $\tfrac{1}{2}.2.2.2$, ou quatre fois de la forme $p^2+q^2$.

2°. Que le produit $5^2.13$ sera $\tfrac{1}{2}.3.2$, ou trois fois de la même forme.

3°. Que le produit $5^2.13^2.17$ sera $\tfrac{1}{2}.3.3.2$, ou neuf fois de cette forme.

4°. Que le produit $5^4.13^4$ sera $\tfrac{1}{2}.5.5$, ou treize fois la somme de deux quarrés ; toutes propositions qu'il est facile de vérifier.

Le problême inverse, qui au premier abord auroit pu paroître fort difficile, se résoudra très-simplement, en faisant attention au résultat trouvé dans la solution directe.

Par exemple, soit proposé de trouver un nombre qui soit trente fois de la forme $p^2+2q^2$. Les nombres les plus simples de cette forme sont les nombres premiers 3, 17, 19, 41, 43, &c., je les désigne par $\alpha, \beta, \gamma$, &c. et le nombre cherché par $\alpha^n \beta^{n'} \gamma^{n''}$ &c.; il faut donc faire en sorte qu'on ait $30=\tfrac{1}{2}(n+1)(n'+1)(n''+1)$&c. Pour cela, décomposez 60 en facteurs, premiers ou non, tels que 3.4.5; diminuez chaque facteur d'une unité, vous aurez 2, 3, 4 pour les valeurs de $n$, $n'$, $n''$. Donc $\alpha^2 \beta^3 \gamma^4$ sera l'un des

nombres cherchés; ainsi $3^4 . 17^3 . 19^2$ doit satisfaire à la question.

Fermat a indiqué cette solution, sans en donner de démonstration, dans une de ses notes sur Diophante, page 128.

Le théorême du n°. 234 dont nous venons de donner diverses applications, renferme une propriété essentielle et très-remarquable des nombres premiers, mais il est susceptible d'être rendu beaucoup plus général, ainsi qu'on va le voir dans les propositions suivantes.

(238) *Tout nombre premier* A *compris dans la formule* $my^2 + nz^2$, *où* m *et* n *sont positifs* (1), *ne peut être exprimé de deux manières différentes par cette formule, en sorte que si l'on a* $A = mf^2 + ng^2$, *on ne pourra avoir en même temps* $A = mf'^2 + ng'^2$, g' *étant différent de* g.

Si on avoit à-la-fois $A = mf^2 + ng^2 = mf'^2 + ng'^2$, il en résulteroit $\frac{f^2 - f'^2}{n} = \frac{g'^2 - g^2}{m}$; équation dont chaque membre doit être un nombre entier, parce que $m$ et $n$ n'ont point de commun diviseur. Soit donc $n = \alpha\zeta$, $m = \gamma\delta$, on pourra faire en général

$$f + f' = \alpha MN \qquad g' + g = \gamma MP$$
$$f - f' = \zeta PQ \qquad g' - g = \delta NQ;$$

ce qui donnera $2f = \alpha MN + \zeta PQ$, $2g = \gamma MP - \delta NQ$; donc $4mf^2 + 4ng^2$ ou $4A = (\alpha\gamma M^2 + \zeta\delta Q^2) . (\alpha\delta N^2 + \zeta\gamma P^2)$.

Maintenant, puisque $A$ est un nombre premier, cette équation ne peut subsister, à moins qu'un des facteurs du second membre ne soit égal à 4 ou à 2.

Soit 1°. $\alpha\gamma M^2 + \zeta\delta Q^2 = 2$ : j'observe qu'aucun des nombres $M$, $N$, $P$, $Q$ ne peut être supposé égal à zéro, parce que cette supposition rendroit identiques les deux formes $mf^2 + ng^2$, $mf'^2 + ng'^2$; on ne pourra donc satisfaire à l'équation précédente qu'en faisant $\alpha\zeta\gamma\delta = 1$; $M = Q = 1$. Mais alors le nombre $A$

(1) Les nombres $m$ et $n$ doivent être premiers entr'eux, puisque $mf^2 + ng^2$ est égal à un nombre premier; mais on peut supposer de plus que $m$ et $n$ n'ont aucun facteur quarré : car si on avoit $m = m'\alpha^2$, il est clair que la formule $my^2 + nz^2$ seroit comprise dans $m'y^2 + nz^2$.

seroit de la forme $y^2+z^2$, et par conséquent il ne pourroit être qu'une fois de cette forme (n°. 234).

Soit 2°. $\alpha\gamma M^2+\beta\delta Q^2=4$, cette équation ne pourra avoir lieu qu'en faisant $\alpha\gamma\beta\delta=3$, $M=Q=1$, alors le nombre $A$ seroit de la forme $y^2+3z^2$, ce qui rentre dans le cas déjà examiné n°. 234.

Donc dans tous les cas le nombre premier $A$ ne pourra être exprimé que d'une manière par la formule $my^2+nz^2$.

(239) *Le double d'un nombre premier* A *ne peut être exprimé non plus de deux manières différentes par la même formule* $my^2+nz^2$, *en sorte que si l'on a* $2A=mf^2+ng^2$, *on ne pourra avoir en même temps* $2A=mf'^2+ng'^2$, $g'$ *étant différent de* $g$.

Car toutes choses restant comme dans la proposition précédente, on sera conduit de même à l'équation

$$8A=(\alpha\gamma M^2+\beta\delta Q^2)(\alpha\delta N^2+\beta\gamma P^2).$$

Or pour que cette équation subsiste, il faut que l'un des facteurs du second membre soit égal à 2, ou à 4, ou à 8, sans cependant qu'aucun des nombres $M$, $N$, $P$, $Q$ soit zéro.

Soit 1°. $\alpha\gamma M^2+\beta\delta Q^2=2$; cette équation ne pourra avoir lieu qu'autant qu'on aura $\alpha\beta\gamma\delta=1$, $M=Q=1$. Mais alors $2A$ seroit de la forme $y^2+z^2$, et si on avoit $2A=f^2+g^2=f'^2+g'^2$, il en résulteroit

$$A=\left(\frac{f+g}{2}\right)^2+\left(\frac{f-g}{2}\right)^2=\left(\frac{f'+g'}{2}\right)^2+\left(\frac{f'-g'}{2}\right)^2$$

Donc le nombre premier $A$ seroit deux fois de la forme $y^2+z^2$, ce qui est impossible (n°. 234).

Soit 2°. $\alpha\gamma M^2+\beta\delta Q^2=4$; la seule manière de satisfaire à cette équation (sans supposer $M$ ou $Q$ égal à zéro, ni $\alpha\beta\gamma\delta$ divisible par un quarré), est de faire $\alpha\beta\gamma\delta=3$, $M=1$, $Q=1$; mais alors on auroit $2A=f^2+3g^2$ équation impossible, parce que le premier membre est de la forme $4n+2$, tandis que le second sera toujours, ou impair, ou multiple de 4.

Soit 3°. $\alpha\gamma M^2+\beta\delta Q^2=8$, il est aisé de voir d'abord que $\alpha\beta\gamma\delta$ ou $mn$ ne peut, dans ce cas, être un nombre pair; car, par exemple, si l'on fait $\alpha\gamma=2$, $\beta\delta=3$, on aura l'équation $2M^2+3N^2=8$,

à laquelle on ne peut satisfaire qu'en faisant $N=0$. Les autres valeurs paires de $mn$ ne pourroient être que 2 ou 10; mais on reconnoîtra de même qu'elles sont inadmissibles.

Il reste donc à examiner les valeurs impaires de $mn$ ou de $\alpha\beta\gamma\delta$, au moins celles qui ne donnent pas plus de 8 pour la somme des deux facteurs $\alpha\gamma+\beta\delta$, car la quantité $\alpha\gamma M^2+\beta\delta Q^2$ est au moins égale à cette somme, puisqu'on ne peut faire ni $M$ ni $Q$ égal à zéro.

Le cas de $mn=1$ ayant été déjà examiné, soit $mn=3$, on aura $M^2+3Q^2=8$, équation dont l'impossibilité est manifeste.

Soit $mn=5$, on aura $M^2+5Q^2=8$, équation pareillement impossible.

Soit $mn=7$, on aura $M^2+7Q^2=8$, équation possible; mais alors on auroit $2A=f^2+7g^2$, équation impossible, parce que le second membre est ou impair ou multiple de 8.

On ne peut faire $mn=9$ à cause du facteur quarré, ni $mn=11$, ou $mn=13$, parce que $1+11$ ou $1+13$ surpassent 8.

Soit enfin $mn=15$, $\alpha\gamma=3$, $\beta\delta=5$, l'équation $3M^2+5Q^2=8$ sera possible; mais alors on auroit $2A=f^2+15g^2$ ou $2A=3f^2+5g^2$, équations toutes deux impossibles, parce que le second membre est ou impair, ou multiple de 8.

Donc, dans aucun cas, le double d'un nombre premier ne peut être compris de deux manières dans la formule $my^2+nz^2$.

(240) *Tout nombre* P *premier, ou double d'un premier, qui est compris dans la formule quadratique* $py^2+2qyz+\pi z^2$, *ne peut être exprimé que d'une manière par cette formule, en sorte que si on a* $P=pf^2+2qfg+2\pi g^2$, *on ne pourra avoir en même temps* $P=pf'^2+2qf'g'+2\pi g'^2$. (On suppose toujours $p$ impair et $2p\pi-q^2$ égal à un nombre positif $c$.)

J'observe d'abord que le cas où $P$ est double d'un nombre premier se ramène aisément à celui où $P$ est un nombre premier; car si on a

$$2A=pf^2+2qfg+2\pi g^2$$
$$2A=pf'^2+2qf'g'+2\pi g'^2,$$

il

il faudra que $f$ et $f'$ soient pairs. Ainsi faisant $f=2h$, $f'=2h'$, on aura

$$A=2ph^2+2qhg+\pi g^2$$
$$A=2ph'^2+2qh'g'+\pi g'^2.$$

Donc s'il est impossible qu'un nombre premier $A$ soit compris de deux manières dans une même formule quadratique, il sera pareillement impossible que son double $2A$ soit exprimé de deux manières par la formule quadratique qui contient $2A$. Réciproquement si la proposition étoit démontrée pour le cas de $P=2A$, elle le seroit pour celui de $P=A$; c'est pourquoi il suffira de considérer l'un de ces cas.

Soit donc $A$ un nombre premier compris dans la formule $py^2+2qyz+2\pi z^2$ qu'on pourra considérer comme l'un des diviseurs quadratiques de la formule $t^2+cu^2$. Si l'on fait $A=pf^2+2qfg+2\pi g^2$, et qu'après avoir déterminé $f^\circ$ et $g^\circ$ par l'équation $fg^\circ-f^\circ g=1$, on substitue $fy+f^\circ z$ et $gy+g^\circ z$ à la place de $y$ et $z$ dans la formule $py^2+2qyz+2\pi z^2$, cette formule deviendra de la forme $Ay^2+2Byz+Cz^2$, où l'on aura $AC-B^2=c$.

Donc si le nombre $A$ est compris de deux manières différentes dans la formule proposée $py^2+2qyz+2\pi z^2$, il faudra qu'on puisse satisfaire à l'équation $A=Ay^2+2Byz+Cz^2$, sans supposer $z=0$. Cette équation étant multipliée par $A$ donne $A^2=(Ay+Bz)^2+cz^2$, ou $A^2-(Ay+Bz)^2=cz^2$. Soit $c=mn$, $m$ et $n$ étant deux facteurs indéterminés, on pourra faire

$$A+Ay+Bz=mM$$
$$A-Ay-Bz=nN,$$

et l'équation à résoudre deviendra $MN=z^2$. Or on satisfait généralement à cette équation, en prenant $M=\lambda\mu^2$, $N=\lambda\nu^2$, $z=\lambda\mu\nu$; $\mu$ et $\nu$ étant premiers entr'eux; on aura donc

$$A+Ay+B\lambda\mu\nu=m\lambda\mu^2$$
$$A-Ay-B\lambda\mu\nu=n\lambda\nu^2,$$

d'où l'on tire $2A=\lambda(m\mu^2+n\nu^2)$.

Ce résultat, qui a lieu quel que soit $A$, prouve que si un nombre quelconque $A$ est compris de deux manières différentes dans une même formule quadratique $py^2+2qyz+2\pi z^2$, son double $2A$

sera le produit de deux facteurs $\lambda$, $\omega$, l'un $\omega$ de la forme $my^2+nz^2$ (où $mn=c$), l'autre $\lambda$ moindre que $\frac{A}{\sqrt{c}}$.

Maintenant si $A$ est un nombre premier, comme on peut faire abstraction du cas de $c=1$, on ne pourra faire ni $\lambda=A$, ni $\lambda=2A$; donc puisque $\lambda$ est diviseur de $2A$, il faudra que $\lambda$ soit 1 ou 2, et ainsi on aura soit $A=m\mu^2+n\nu^2$, soit $2A=m\mu^2+n\nu^2$.

1°. Si on a $A=m\mu^2+n\nu^2$, le nombre premier $A$ sera compris dans la formule $my^2+nz^2$, qui est l'un des diviseurs quadratiques de la formule $t^2+cu^2$. Mais comme un même nombre premier ne sauroit appartenir à deux différens diviseurs quadratiques d'une même formule $t^2+cu^2$, il s'ensuit que la formule $my^2+nz^2$ doit coincider avec la formule donnée $py^2+2qyz+2\pi z^2$. Or on a prouvé (n°. 238) que le nombre premier $A$ ne peut être qu'une fois de la forme $my^2+nz^2$, donc il ne peut être qu'une fois (1) de la forme équivalente $py^2+2qyz+2\pi z^2$.

2°. Si on a $2A=my^2+nz^2$, le nombre $2A$ appartiendra au diviseur quadratique $my^2+nz^2$. Mais de ce que le nombre $A$ est compris dans le diviseur $py^2+2qyz+2\pi z^2$, il s'ensuit que $2A$ est compris dans le diviseur conjugué $2py^2+2qyz+\pi z^2$. Donc comme $2A$ ne peut appartenir à deux diviseurs quadratiques différens, il faut que la formule $2py^2+2qyz+\pi z^2$ soit identique avec $my^2+nz^2$. Mais s'il y avoit deux solutions de l'équation $A=py^2+2qyz+2\pi z^2$, il y en auroit deux de l'équation $2A=2py^2+2qyz+\pi z^2$, et partant deux de son identique $2A=my^2+nz^2$, ce qui est impossible (n°. 239).

Donc le nombre premier $A$ ne peut être exprimé de deux manières différentes par la même formule $py^2+2qyz+2\pi z^2$; *donc tout nombre* P, &c.

(241) *Remarque.* Cette proposition générale est cependant sujette à deux exceptions, lorsqu'on a $q=p$ ou $q=\pi$.

1°. Si le nombre $P$ est compris dans la formule $py^2+2pyz+2\pi z^2$,

(1) Cette conclusion est sujette à une exception dont il sera fait mention dans la Remarque suivante.

on pourra, sans changer $z$, mettre $-y-2z$ à la place de $y$, et ainsi il y aura toujours deux solutions de l'équation $P=py^2+2pyz+2\pi z^2$. Mais alors on peut réduire la formule dont il s'agit à la forme $my^2+nz^2$; et dans celle-ci les deux solutions se réduisent à une seule, de sorte que l'exception n'est qu'apparente, et peut être totalement évitée, en mettant la formule proposée sous une forme plus simple.

2°. Si le nombre $P$ est compris dans la formule $py^2+2qyz+2qz^2$, on pourra, sans changer $y$, mettre $-y-z$ à la place de $z$, ce qui donnera deux solutions de l'équation $P=py^2+2qyz+2qz^2$. Mais j'observe que selon que $P$ est égal au nombre premier $A$ ou à son double, les nombres $2A$ ou $A$ se réduiront à la forme $my^2+nz^2$, et les deux solutions à l'égard de cette dernière forme coincideront en une seule.

Un troisième cas où l'on auroit $P=py^2+2qyz+pz^2$ paroît devoir faire exception, puisqu'il est évident qu'on peut permuter $y$ et $z$ entr'eux, sans changer la valeur de $P$; mais ce cas est compris dans le précédent, parce que si à la place de $y$ on met $y-z$, la formule $py^2+2qyz+pz^2$ aura pour transformée $py^2-(2p-2q)yz+(2p-2q)z^2$, où le coefficient de $yz$ est égal à celui de $z^2$.

On voit par conséquent que les exceptions à la proposition générale se réduisent au seul cas où l'on a $P=py^2+2qyz+2qz^2$; et cette exception est encore limitée, de manière que des deux nombres $A$, $2A$, l'un seulement exprimé par cette formule y sera compris de deux manières, tandis que l'autre compris dans la formule $my^2+nz^2$ ne sera susceptible que d'une seule forme.

(242) *Tout nombre premier* A *compris dans la formule quadratique* $py^2+qyz+rz^2$ *dont les coefficiens sont impairs, n'y peut être compris que d'une seule manière, excepté dans le cas évident où deux des nombres* p, q, r *sont égaux.* (On suppose toujours $4pr-q^2$ égal à un nombre positif $c$.)

On a déjà vu, n°. 219, que la formule $py^2+qyz+rz^2$ renferme les trois suivantes :

$$py^2+2qyz+4rz^2$$

$$4py^2+2qyz+rz^2$$
$$(p-q+r)y^2+(4p-2q)yz+4pz^2,$$

donc il faudra que le nombre premier $A$ appartienne à l'une de ces formules. Mais celles-ci étant réduites à la forme ordinaire, où deux coefficiens sont pairs, il suit du théorême précédent, que le nombre $A$ ne pourra être compris que d'une seule manière dans la formule à laquelle il appartient; donc il ne pourra être exprimé que d'une manière par la formule proposée $py^2+qyz+rz^2$, sauf les cas prévus qu'il faut examiner.

1°. Si l'on a $q=p$, les trois formules comprises dans $qy^2+qyz+rz^2$ se réduisent aux deux suivantes :

$$qy^2+2qyz+4rz^2$$
$$4qy^2+2qyz+\ rz^2.$$

Mais la première peut se réduire ultérieurement à la forme $qy^2+(4r-q)z^2$, donc alors le nombre $A$ sera ou de la forme $qy^2+(4r-q)z^2$, ou de la forme $4qy^2+2qyz+rz^2$, et dans les deux cas, il ne peut être représenté que d'une manière par ces formules, quoiqu'il le puisse être de deux par la formule proposée $qy^2+qyz+rz^2$.

2°. Le cas de $q=r$ donnera un résultat semblable.

3°. Si l'on a $p=r$, les trois formules comprises dans $py^2+qyz+pz^2$ se réduisent aux deux suivantes :

$$py^2+2qyz+4pz^2$$
$$(2p-q)y^2+(4p-2q)yz+4pz^2.$$

La dernière est la seule qui puisse donner lieu à exception; mais comme elle peut être mise sous la forme $(2p-q)y^2+(2p+q)z^2$, il s'ensuit que le nombre $A$, qui doit être compris dans l'une ou l'autre de ces deux formes, n'y pourra être compris que d'une seule manière.

On voit par ces détails, que les cas d'exception résultans de l'égalité entre deux des coefficiens $p$, $q$, $r$, n'existent plus lorsqu'on réduit la formule proposée aux formes les plus simples dont elle est susceptible; de sorte qu'alors le nombre premier $A$ ne peut s'exprimer que d'une manière par celle des formules réduites à laquelle il appartient.

Par exemple, le nombre 23 résulte de la formule $3y^2+3yz+5z^2$, soit en faisant $z=1$, $y=2$, soit en faisant $z=1$, $y=-3$; mais le même nombre 23 n'est compris que d'une seule manière dans la formule $12y^2+6yz+5z^2$, l'une des deux dans lesquelles se résout la formule donnée $3y^2+3yz+5z^2$.

*Nota.* Les théorêmes précédens concernant les nombres $P=A$, $P=2A$, premiers ou doubles de premiers, s'appliquent également aux nombres de la forme $P=A^k$, $P=2A^k$, $k$ étant un exposant quelconque; car dans ces formes, comme dans celles où $k=1$, le nombre $P$ ne pourra appartenir qu'à un seul diviseur quadratique de la formule $t^2+cu^2$ (Voyez n°. 232).

(243) *Soit* P *un nombre composé, impair ou double d'un impairs, si l'on suppose que* P *soit diviseur de la formule* $t^2+cu^2$, *et qu'en conséquence* P *soit compris dans un ou plusieurs diviseurs quadratiques de cette formule, je dis que* P *sera toujours exprimé par ces diviseurs quadratiques de* $2^{i-1}$ *manières différentes*, i *étant le nombre des facteurs premiers inégaux qui divisent* P *sans diviser* c.

En effet, puisque $P$ est diviseur de la formule $t^2+cu^2$, il le sera de la formule $x^2+c$, et l'équation $\frac{x^2+c}{P}=e$ aura autant de solutions qu'il y a d'unités dans $2^{i-1}$ (voyez n°. 191). Soient $Q$, $Q'$, $Q''$, &c., ces différentes valeurs de $x$ moindres que $\frac{1}{2}P$, et soient en même temps $R$, $R'$, $R''$, &c. les valeurs correspondantes de la quantité $\frac{x^2+c}{P}$, on pourra avec ces nombres composer les formules

$$Py^2+2Qyz+Rz^2$$
$$Py^2+2Q'yz+R'z^2$$
$$Py^2+2Q''yz+R''z^2$$
&c.

dans lesquelles $P$ est constamment le même, et qui seront toutes des diviseurs quadratiques de la formule $t^2+cu^2$.

Soit $py^2+2qyz+rz^2$ un des diviseurs de la même formule, réduit à la forme la plus simple, et dans lequel le nombre $P$ soit

contenu, on pourra donc supposer $P = pf^2 + 2qfg + rg^2$. Si ensuite on détermine $f^\circ$ et $g^\circ$ d'après l'équation $fg^\circ - f^\circ g = 1$, et qu'on mette $fy + f^\circ z$ au lieu de $y$, et $gy + g^\circ z$ au lieu de $z$, la formule $py^2 + 2qyz + rz^2$ devieudra par cette substitution $Py^2 + 2Myz + Nz^2$, et on aura

$$M = pff^\circ + q(fg^\circ + f^\circ g) + rgg^\circ$$
$$N = pf^{\circ 2} + 2qf^\circ g^\circ + rg^{\circ 2}.$$

D'ailleurs on pourra toujours preudre $f^\circ$ et $g^\circ$ de manière que $M$ soit moindre ou non plus grand que $\frac{1}{2}P$. De-là on voit que pour que $M$ puisse être successivement égal à chacun des nombres $Q$, $Q'$, $Q''$, &c. (comme cela est nécessaire, puisque chaque diviseur quadratique $Py^2 + 2Qyz + Rz^2$, après avoir été réduit à la forme la plus simple, doit coincider avec l'un des diviseurs représentés par $py^2 + 2qyz + rz^2$) il faut que les valeurs de $f$ et $g$ puissent être variées en autant de manières qu'il y a de nombres $Q$, $Q'$, $Q''$, &c., c'est-à-dire en un nombre de manières $2^{i-1}$, $i$ étant le nombre des facteurs premiers, inégaux et impairs, qui divisent $P$ sans diviser $c$.

Donc le nombre $P$ sera compris de $2^{i-1}$ manières différentes dans les diviseurs quadratiques de la formule $t^2 + cu^2$.

(244) Si le diviseur quadratique $py^2 + 2qyz + rz^2$, est le seul affecté à un même groupe de diviseurs linéaires, il faudra que les $2^{i-1}$ formes dont il vient d'être question soient comprises dans ce seul diviseur, et ainsi il y aura dans ce cas $2^{i-1}$ manières de satisfaire à l'équation $P = py^2 + 2qyz + rz^2$. Résultat remarquable, et qui mérite d'être confirmé par un exemple.

La formule $t^2 + 69u^2$ a pour diviseurs, d'après la Table IV, les nombres premiers 5, 7, 13, 17, 19, &c.; donc le produit 5.7.19, par exemple, ou 595, est un diviseur de la même formule. Ce diviseur étant de la forme $276x + 43$, la même Table fait voir qu'il doit être compris dans le diviseur quadratique $10y^2 + 2yz + 7z^2$, et parce que ce diviseur est seul de son espèce, et qu'en même temps le nombre compris 595 est composé de trois facteurs impairs, inégaux, il faudra, d'après le corollaire précédent, que 595 soit compris de $2^{3-1}$ ou 4 manières dans la formule $10y^2 + 2yz + 7z^2$.

En effet, si on met l'équation $595 = 10y^2 + 2yz + 7z^2$ sous cette forme $(10y+z)^2 = 5950 - 69z^2$, et qu'on donne à $z$ les valeurs successives 0, 1, 2, 3, &c., on trouvera les solutions suivantes :

$$z=3,\ 10y+z=\pm 73,\ y=7$$
$$z=5,\ 10y+z=\pm 65,\ y=\begin{cases}6\\-7\end{cases}$$
$$z=9,\ 10y+z=\pm 19,\ y=1.$$

Donc il y a trois valeurs de $z$ dont une répond à deux valeurs de $y$, et ainsi il y a quatre solutions de l'équation proposée, conformément au théorême.

(245) *Remarque I.* Les mêmes exceptions qui ont été observées n°. 241, lorsque $P$ est premier ou double d'un nombre premier, ont également lieu lorsque $P$ est un nombre composé ; mais on peut les éviter de manière que le résultat réponde exactement à l'énoncé du théorême.

Ces exceptions se réduisent aux deux cas où l'on auroit $P = qy^2 + 2qyz + rz^2$, ou $P = py^2 + 2qyz + 2qz^2$; or dans le premier cas on peut mettre $P$ sous la forme $P = qy^2 + (r-q)z^2$, et il n'y a plus lieu à exception. Dans le second, on peut écrire $2P = (2p-q)y^2 + qz^2$, si $P$ est impair, et $P = 2(qz^2 + (2p-q)y^2)$ si $P$ est pair ; dans ces dernières formes, il n'y aura plus que le nombre de solutions désigné par $2^{i-1}$. On peut aussi, dans le second cas, ne pas regarder comme différentes la solution $y = \alpha$, $z = \zeta$, et la solution $y = \alpha$, $z = -\alpha - \zeta$.

*Remarque II.* Si un nombre impair $P$ est diviseur de la formule $t^2 + cu^2$, où $c$ est de forme $8n+3$, et qu'en conséquence $P$ soit compris dans le diviseur quadratique $py^2 + qyz + rz^2$ dont les coefficiens sont impairs, on prouvera, comme ci-dessus, que le nombre $P$ sera compris, de $2^{i-1}$ manières différentes, dans les diviseurs quadratiques de la formule $t^2 + cu^2$, $i$ étant le nombre de facteurs premiers inégaux qui divisent $P$ sans diviser $c$.

L'exception qui auroit lieu, si on avoit $r = q$, peut être évitée de deux manières, 1°. en considérant comme une même solution celles qui donnent les mêmes valeurs tant pour $y$ que pour $(y+z)z$, 2°. en considérant, au lieu des valeurs de $P$, celles de $4P$ comprises dans la formule $4P = (4p-q)y^2 + qz^2$.

## §. XIV. *Sur les moyens de trouver un nombre premier plus grand qu'un nombre donné.*

(246) Soit $M$ un nombre contenu deux ou plusieurs fois dans la formule $py^2+2qyz+rz^2$, en sorte qu'on ait

$$M=p\alpha^2+2q\alpha\zeta+r\zeta^2=p\gamma^2+2q\gamma\delta+r\delta^2;$$

multipliant tout par $p$, et faisant à l'ordinaire $pr-q^2=c$, on aura

$$(p\alpha+q\zeta)^2+c\zeta^2=(p\gamma+q\delta)^2+c\delta^2.$$

Supposons que $c$ ou $\frac{1}{2}c$ soit un nombre premier, ou qu'au moins si l'un ou l'autre est le produit de deux facteurs, l'un de ces facteurs soit commun avec $p$ et $q$; alors l'équation précédente ne peut avoir lieu, à moins que $p\alpha+q\zeta\pm(p\gamma+q\delta)$ ne soit divisible par $c$. Soit donc $p\gamma+q\delta=\pm(p\alpha+q\zeta-cx)$, on aura, après avoir substitué et divisé par $c$, l'équation

$$\zeta^2+2(p\alpha+q\zeta)x-cx^2=\delta^2. \qquad \text{(a)}$$

Toutes les fois que cette équation sera possible, c'est-à-dire, toutes les fois qu'on pourra trouver une valeur de $x$ autre que zéro, par laquelle le premier membre devienne un quarré parfait, il s'ensuivra que le nombre $M$ ou sa moitié n'est pas un nombre premier.

(247) Si l'équation (a) n'est possible qu'en faisant $x=0$, il ne faudra pas encore en conclure que le nombre $M$ ou sa moitié est un nombre premier. Cependant si dans ce même cas le diviseur quadratique $py^2+2qyz+rz^2$ relatif à la formule $t^2+cu^2$, est seul de son espèce, en sorte qu'un nombre qui y est contenu ne puisse appartenir à aucun autre diviseur quadratique de la même formule $t^2+cu^2$; ou en d'autres termes, si le diviseur quadratique $py^2+2qyz+rz^2$ est seul affecté à un même groupe de diviseurs linéaires, comme on en voit des exemples multipliés dans les Tables IV, V, VI et VII, je dis qu'on pourra conclure que le nombre $M$ ou sa moitié est un nombre premier, sauf une exception dont il sera fait mention.

En

En effet, 1°. si le nombre $M$, compris dans la formule $py^2+2qyz+rz^2$, est divisible par deux nombres premiers différens non diviseurs de $c$, on a déjà vu (n°. 244) que $M$ sera compris de deux manières différentes dans la formule $py^2+2qyz+rz^2$, puisque celle-ci est seule de son espèce. Donc alors l'équation (a) auroit au moins deux solutions.

2°. Si le nombre $M$ est égal à une puissance paire du nombre premier $\alpha$, ou si l'on a $M=\alpha^{2m}$, alors le nombre $M$ appartiendra au diviseur quadratique $y^2+cz^2$; car si dans ce diviseur on fait $y=\alpha^m$ et $z=$ à un nombre pair, on obtiendra la même forme linéaire $4cx+a$ qui convient au nombre $M$. Mais on suppose que les formes linéaires dans lesquelles $M$ est compris ne répondent qu'à un seul diviseur quadratique $py^2+2qyz+rz^2$; donc ce diviseur, dans lequel $M$ est contenu, n'est autre que $y^2+cz^2$, ou son équivalent $y^2+2yz+(c+1)z^2$. J'observe maintenant que le nombre $M$ qui sera exprimé par $f^2+cg^2$, $f$ et $g$ étant premiers entr'eux, pourra l'être aussi par la simple formule $\gamma^2$, en faisant $y=\gamma=\alpha^m$, $z=0$; et quoique cette dernière expression ne soit pas régulière, puisqu'on doit toujours supposer $y$ et $z$ premiers entr'eux, cependant il n'en est pas moins vrai qu'on pourra faire $f^2+cg^2=\gamma^2$, et qu'ainsi l'équation (a), outre la solution $x=0$, en aura une autre qui donne $\delta=0$.

3°. Si le nombre $M=\alpha^{2m+1}$, $\alpha$ étant un nombre premier, alors il est aisé de voir que $\alpha$ et $M$ appartiendront au même diviseur quadratique. Car soit $\alpha y^2+2\zeta yz+\gamma z^2$ le diviseur quadratique qui contient $\alpha$, si l'on fait $y=\alpha^m$ et $z$ égal à un multiple de $2c$, alors ce diviseur devient de la même forme linéaire $4cx+a$ dont est $\alpha^{2m+1}$ ou $M$. Mais il n'y a par supposition qu'un seul diviseur quadratique qui réponde au groupe de formes linéaires dans lequel $M$ est compris, donc ce diviseur $py^2+2qyz+rz^2$ sera identique avec le diviseur $\alpha y^2+2\zeta yz+\gamma z^2$. Or celui-ci offrira toujours deux manières de représenter $M$, l'une où $y$ et $z$ seroient premiers entr'eux, l'autre où l'on feroit $y=\alpha^m$, $z=0$. Donc, en vertu de ces deux expressions, l'équation (a) auroit encore deux solutions.

4°. Si on a $M=\alpha^{2m}$, on prouvera, d'une manière semblable, que le nombre $M$ appartiendra au diviseur quadratique

$2y^2+2yz+\left(\frac{c+1}{2}\right)z^2$, si $c$ est impair, ou au diviseur $2y^2+\frac{c}{2}z^2$, si $c$ est pair. Dans les deux cas, le nombre $M$ pourra être exprimé de deux manières par ce diviseur, et ainsi l'équation (a) aura deux solutions.

5°. Si le nombre $M=2\alpha^{2m+1}$, on prouvera encore de la même manière, que le nombre $M$ appartiendra au même diviseur quadratique que $2\alpha$, et qu'ainsi ce diviseur pourra être représenté par $2\alpha y^2+2\mathcal{C}yz+\gamma z^2$. Il y aura donc au moins deux manières de satisfaire à l'équation $M=py^2+2qyz+rz^2$, et par conséquent au moins deux solutions de l'équation (a).

Il paroît, par l'examen de tous ces cas, que si le premier membre de l'équation (a) ne peut devenir un quarré que lorsque $x=0$, on peut conclure que le nombre $M$ ou $\frac{1}{2}M$ est un nombre premier. Il faut néanmoins excepter le cas où $M$ auroit un facteur premier $\alpha$ non commun avec $c$, et plusieurs autres $\mathcal{C}$, $\gamma$, &c. communs avec $c$, car alors l'équation $\frac{x^2+c}{M}=e$ ne seroit susceptible que d'une solution, et le nombre $M$ ne pourroit être représenté que d'une manière par la formule $py^2+2qyz+rz^2$. Mais si d'une part le diviseur quadratique $py^2+2qyz+rz^2$ qui contient $M$ est seul de son espèce; si d'autre part $M$ n'a aucun diviseur commun avec $c$, et que la quantité $\mathcal{C}^2+2(p\alpha+q\mathcal{C})x-cx^2$, formée d'après la valeur $M=p\alpha^2+2q\alpha\mathcal{C}+r\mathcal{C}^2$, ne puisse être égale à un quarré que dans le seul cas de $x=0$, on pourra conclure avec certitude de ces conditions réunies, que le nombre $M$ ou sa moitié, s'il est pair, est un nombre premier.

(248) Cela posé, si on prend pour $\alpha$ et $\mathcal{C}$ des nombres quelconques premiers entr'eux, on pourra regarder comme autant de Théorêmes les résultats suivans choisis entre plusieurs autres semblables qui sont contenus dans nos Tables. Ils indiquent diverses formules générales dans lesquelles tout nombre compris sera premier ou double d'un premier, si la formule conditionnelle ne peut être un quarré que lorsque $x=0$, et si en même temps $M$ et $c$ sont premiers entr'eux, ainsi que $\alpha$ et $\mathcal{C}$.

| *Formule conditionnelle.* | *Formule de nombres premiers.* |
|---|---|
| $\beta^2+2(\alpha+\beta)x-13x^2$ | $\alpha^2+2\alpha\beta+14\beta^2$ |
| $\beta^2+2(\alpha+\beta)x-37x^2$ | $\alpha^2+2\alpha\beta+38\beta^2$ |
| $\beta^2+6(\alpha+\beta)x-57x^2$ | $3\alpha^2+6\alpha\beta+22\beta^2$ |
| $\beta^2+6(\alpha+\beta)x-93x^2$ | $3\alpha^2+6\alpha\beta+34\beta^2$ |
| $\beta^2+6(5\alpha+\beta)x-141x^2$ | $15\alpha^2+6\alpha\beta+10\beta^2$ |
| $\beta^2+2(11\alpha+7\beta)x-193x^2$ | $11\alpha^2+14\alpha\beta+22\beta^2$ |
| $\beta^2+2(2\alpha+\beta)x-11x^2$ | $\alpha^2+\alpha\beta+3\beta^2$ |
| $\beta^2+2(2\alpha+\beta)x-19x^2$ | $\alpha^2+\alpha\beta+5\beta^2$ |
| $\beta^2+2(2\alpha+\beta)x-43x^2$ | $\alpha^2+\alpha\beta+11\beta^2$ |
| $\beta^2+2(2\alpha+\beta)x-67x^2$ | $\alpha^2+\alpha\beta+17\beta^2$ |
| $\beta^2+6(2\alpha+\beta)x-123x^2$ | $3\alpha^2+3\alpha\beta+11\beta^2$ |
| $\beta^2+2(2\alpha+\beta)x-163x^2$ | $\alpha^2+\alpha\beta+41\beta^2$ |
| $\beta^2+10(2\alpha+\beta)x-235x^2$ | $5\alpha^2+5\alpha\beta+13\beta^2$ |
| $\beta^2+2\alpha x-10x^2$ | $\alpha^2+10\beta^2$ |
| $\beta^2+2\alpha x-22x^2$ | $\alpha^2+22\beta^2$ |
| $\beta^2+2\alpha x-58x^2$ | $\alpha^2+58\beta^2$ |
| $\beta^2+10\alpha x-70x^2$ | $5\alpha^2+14\beta^2$ |
| $\beta^2+6\alpha x-102x^2$ | $3\alpha^2+34\beta^2$ |
| $\beta^2+10\alpha x-190x^2$ | $5\alpha^2+38\beta^2$ |

(249) Si l'on supposoit les nombres $\beta$, $\gamma$, $c$ pris au hasard, il seroit facile de trouver combien il est probable que la formule $\beta^2+2\gamma x-cx^2$ deviendra un quarré, en prenant pour $x$ un nombre entier quelconque positif ou négatif, excepté zéro. En effet, puisque $n^2$ est le seul quarré contenu entre les limites $n^2-n+\frac{1}{4}$, $n^2+n+\frac{1}{4}$, il s'ensuit que $\frac{1}{2\sqrt{A}}$ est la probabilité qu'un nombre $A$ pris au hasard sera un quarré. Et d'après ce principe, on trouvera aisément que la probabilité de ne rencontrer aucun quarré dans toutes les valeurs de $\beta^2+2\gamma x-cx^2$, est égale au produit de toutes les quantités $1-\frac{1}{2\sqrt{(\beta^2+2\gamma x-cx^2)}}$ formées en donnant à $x$ toutes les valeurs en nombres entiers, positifs ou négatifs (zéro excepté) comprises entre les deux racines de l'équation

$\zeta^2+2\gamma x-cx^2=0$. Donc si le nombre $\zeta^2+2\gamma x-cx^2$ reste toujours assez grand (1), la probabilité contraire, ou celle de rencontrer un quarré, sera sensiblement égale à la somme de toutes les quantités $\frac{1}{2\sqrt{(\zeta^2+2\gamma x-cx^2)}}$. Mais au moyen du cercle dont l'équation est $y^2=\frac{\zeta^2}{c}+\frac{2\gamma x}{c}-x^2$, il est facile de voir que cette somme est à-peu-près $\frac{\pi}{2\sqrt{c}}$, $\pi$ désignant le rapport de la circonférence au diamètre; donc $\frac{\pi}{2\sqrt{c}}$ sera une valeur approchée de la probabilité dont il s'agit (2).

Ce résultat dépend seulement de $c$, et il est d'autant plus petit, que $c$ est plus grand. De-là il est facile de juger quelles sont les formules qui sont les plus propres à donner des nombres premiers.

Par exemple, ponr que la quantité $\zeta^2+2(2\alpha+\zeta)x-163x^2$ devienne un quarré, la probabilité est $\frac{\pi}{2\sqrt{163}}$ ou à-peu-près $\frac{1}{8}$. Donc il y a environ 7 à parier contre 1, que le nombre $\alpha^2+\alpha\zeta+41\zeta^2$ sera un nombre premier, $\alpha$ et $\zeta$ étant pris au hasard parmi les nombres premiers entr'eux.

Il y auroit près de 8 à parier contre 1, qne la formule $5\alpha^2+38\zeta^2$ donnera un nombre premier, ou le double d'un tel nombre, $\alpha$ et $\zeta$ étant pris à volonté premiers entr'eux, et en supposant que $\alpha$ n'est point divisible par 19, ni $\zeta$ par 5.

Ces deux formules, et sur-tout la dernière, sont celles de toute

---

(1) Les résultats que nous indiquons ne seroient pas exacts, si la quantité $\zeta^2+2\gamma x-cx^2$ pouvoit être égale à zéro. Mais dans la formule dont il s'agit, où l'on a $\gamma=p\alpha+q\zeta$, cette égalité ne peut avoir lieu, parce qu'il en résulteroit $cx=p\alpha+q\zeta\pm\sqrt{pM}$, donc il faudroit que $pM$ fût un quarré. Or ce cas est l'un de ceux qu'on peut vérifier d'avance, et mettre à l'écart, comme ne pouvant donner pour $M$ ou $\frac{1}{2}M$ un nombre premier.

(2) Cette estimation ne doit pas être prise à la rigueur, elle n'est employée ici que comme un moyen grossier de comparer deux formules quant à leur aptitude à contenir des nombres premiers.

la Table qui présentent le plus d'avantages pour la détermination d'un nombre premier plus grand qu'un nombre donné.

(250) Pour s'assurer si la quantité $\beta^2+2(p\alpha+q\beta x-cxx$ ne peut être un quarré que lorsque $x=0$, il faudra essayer pour $x$ toutes les valeurs en nombres entiers comprises entre les deux racines de l'équation $\beta^2+2(p\alpha+q\beta)x-cxx=0$. Le nombre des essais est donc en général $\frac{2}{c}\sqrt{pM}$, $M$ étant le nombre $p\alpha^2+2q\alpha\beta+r\beta^2$ dont on veut déterminer la nature. La formule la plus avantageuse, ou celle qui exige le moins d'essais, est donc celle où, toutes choses d'ailleurs égales, $p$ sera le plus petit, et $c$ le plus grand.

Par exemple, si on considère la formule $\alpha^2+\alpha\beta+41\beta^2$, ou plutôt $2\alpha^2+2\alpha\beta+82\beta^2$, afin de l'assimiler à la formule générale $py^2+2qyz+rz^2$, le nombre des essais, pour s'assurer si le nombre $N=\alpha^2+\alpha\beta+41\beta^2$ est un nombre premier, sera $\frac{4\sqrt{N}}{163}$, ou à-peu-près $\frac{1}{41}\sqrt{N}$.

La formule $5\alpha^2+38\beta^2$, qui répond au nombre $c=190$, est encore plus avantageuse, au moins en prenant $\alpha$ impair; car si l'on fait $N=5\alpha^2+38\beta^2$, le nombre des essais sera $\frac{2\sqrt{5N}}{190}$ ou $\frac{2}{85}\sqrt{N}<\frac{4}{163}\sqrt{N}$. Si l'on suppose de plus dans cette seconde formule, que le nombre $\beta$ soit impair, le nombre des essais se réduira encore à moitié. En effet, si $\beta$ est impair, ainsi que $\alpha$, la quantité $\beta^2+10\alpha x-190x^2$ ne pourra être de la forme $8n+1$, ni par conséquent devenir un quarré, à moins qu'on ne suppose $x$ de la forme $4k$ ou $4k-\alpha$, et ainsi les formes $4k+2$, $4k-\alpha$ étant exclues, le nombre des essais se réduit à $\frac{1}{85}\sqrt{N}$.

(251) Enfin on peut observer que plus $\alpha$ sera petit, plus la limite de $x$ sera petite. D'après toutes ces considérations, voici la manière qui paroît la plus simple de trouver un nombre premier plus grand qu'une limite donnée $L$.

Ayant fait $\alpha=1$, prenez pour $\beta$ un nombre impair $>\sqrt{\frac{L}{38}}$ et

non divisible par 5, vous aurez le nombre impair $N = 5 + 38c^2$ plus grand que la limite donnée $L$; ce nombre n'a point de diviseur commun avec 190; donc pour savoir si $N$ est un nombre premier, il restera à examiner s'il y a une valeur de $x$ autre que zéro qui puisse rendre la quantité $c^2 + 10x - 190x^2$ égale à un quarré. Les valeurs de $x$ à essayer seront tous les nombres de forme $4k$ ou $4k-1$, tant positifs que négatifs, moindres que $\frac{c}{\sqrt{190}}$ : si aucun de ces nombres ne rend la quantité dont il s'agit égale à un quarré, on en conclura que le nombre $5 + 38c^2$ est un nombre premier.

Soit proposé, par exemple, de trouver par cette méthode un nombre premier plus grand que 1000000; on prendra $c$ impair et $> \sqrt{\frac{1000000}{38}}$. Soit $c = 163$, il faudra voir si on peut satisfaire à l'équation

$$26569 + 10x - 190x^2 = y^2.$$

Les valeurs de $x$ à essayer seront seulement $-1, 3, \pm 4, -5, 7, \pm 8, -9, 11$; et comme aucune d'elles ne rend le premier membre égal à un quarré, il s'ensuit que le nombre $5 + 38c^2 = 1009627$ est un nombre premier.

(252) Dans des exemples plus compliqués, on parviendroit facilement à diminuer encore le nombre des tentatives, en observant quels sont les restes des quarrés divisés par 3, par 7, ou par quelqu'autre nombre premier, et excluant les valeurs de $x$ qui ne peuvent donner ces restes. Ainsi, en prenant $c = 3h$, on trouveroit que $x$ ne peut avoir aucune des quatre formes $9k+3$, $9k+4$, $9k+6$, $9k+7$, ce qui réduit le nombre des essais aux $\frac{5}{9}$ du nombre total. Si l'on avoit $c = 22h \pm 1$, les formes exclues seroient $x = 11k + 1, 6, 8, 9, 10$, et le nombre des essais seroit réduit aux $\frac{6}{11}$. Donc par la combinaison de deux semblables suppositions, c'est-à-dire en prenant $c = 66k \pm 21$, le nombre des valeurs de $x$ à essayer se réduiroit à $\frac{5}{9}.\frac{6}{11}$ ou $\frac{10}{33}$ du nombre total qui est environ $\frac{1}{85}\sqrt{L}$, et deviendroit seulement $\frac{1}{280}\sqrt{L}$.

Soit, par exemple, $c = 681$; pour savoir si le nombre $5 + 38c^2$

$= 17\,612\,923$ est un nombre premier, il faut voir si on peut satisfaire à l'équation $463761 + 10x - 190x^2 = y^2$; et d'après ce que nous venons de trouver, les valeurs de $x$ à essayer se réduisent aux suivantes :

$$11, 27, 35, 36, 44, 47, -4, -8, -9, -17, -28, -37, -40, -44.$$

Or la valeur 35 donne $y = 481$, donc le nombre dont il est question n'est pas un nombre premier.

Soit encore $\zeta = 747$, on aura la quantité $558009 + 10x - 190x^2$ dans laquelle il faudra substituer pour $x$ chacun des nombres suivans :

$$11, 27, 35, 36, 44, 47, -4, -8, -9, -17, -28, -37, -40, -44, -52, -53.$$

Et comme on trouve qu'aucun de ces nombres ne rend la quantité dont il s'agit égale à un quarré, il s'ensuit que le nombre $5 + 38\zeta^2 = 21\,204\,347$ est un nombre premier.

(253) On peut, d'après ces principes, expliquer d'une manière satisfaisante, pourquoi certaines formules renferment une suite de nombres premiers assez étendue. (Voyez Introd. n°. XVI.)

Par exemple, on trouve dans la Table (n°. 248) que la formule $\alpha^2 + \alpha + 41$ doit être égale à un nombre premier, toutes les fois que la quantité $1 + (4\alpha + 2)x - 163x^2$ ne pourra devenir un quarré qu'en faisant $x = 0$. Or on voit au premier coup d'œil, que cette quantité ne pourra être un quarré, ni même un nombre positif, tant que $4\alpha + 2$ sera $< 163$, ou $\alpha < 40$. Donc si on fait successivement $\alpha = 0, 1, 2, 3\ldots$ jusqu'à 39, toutes les valeurs qui en résulteront pour $\alpha^2 + \alpha + 41$, doivent être des nombres premiers.

On trouve également, dans la Table du n°. 248, que la formule $\alpha^2 + 58$ désigne un nombre premier ou son double, toutes les fois que $1 + 2\alpha x - 58x^2$ ne pourra être un quarré (excepté en faisant $x = 0$). Or il est manifeste que cette quantité ne peut être un quarré tant que $\alpha$ sera au-dessous de 29. On voit donc *a priori* que les 29 premiers nombres contenus dans la formule $\alpha^2 + 58$ doivent être premiers ou doubles de premiers.

Il en est de même des 19 premiers nombres contenus dans la

formule $5a^2+38$, parce que la quantité $1+10ax-190x^2$ ne peut devenir un quarré, tant que $a$ est au-dessous de 19.

*Remarque.* Le problême de déterminer un nombre premier plus grand qu'un nombre donné, n'est pas résolu complètement dans ce paragraphe. On a indiqué seulement diverses formules, dans lesquelles prenant au hasard un nombre plus grand que la limite assignée, il y a déjà une probabilité assez grande que ce nombre sera premier. Mais pour s'en assurer entièrement, il faut faire des essais qui sont d'autant plus longs, que le nombre dont il s'agit doit être plus considérable; et si cette grandeur passe certaines limites, il pourra être plus avantageux de suivre les méthodes indiquées dans le paragraphe suivant.

---

§. XV.

## §. XV. *Usage des Théorêmes précédens pour reconnoître si un nombre donné est premier ou s'il ne l'est pas.*

(254) Les Tables de nombres premiers qu'on a construites jusqu'à présent n'étant pas fort étendues, il seroit à desirer, pour la perfection de la théorie des nombres, qu'on trouvât une méthode praticable au moyen de laquelle on pût décider assez promptement si un nombre donné qui excède les limites des Tables est premier ou s'il ne l'est pas. En attendant que cette méthode soit trouvée, nous allons faire voir quels secours on peut tirer des théorêmes exposés jusqu'à présent, pour la solution de ce problême particulier.

On a déjà vu que si le nombre proposé $A$ est de la forme $a^n \pm 1$, ou s'il est seulement diviseur de cette formule, tout nombre premier qui divise $A$ doit être de la forme $nx+1$ ou $2nx+1$ lorsque $n$ est impair; car s'il n'étoit pas de cette forme, il diviseroit le nombre plus petit $a^\nu \pm 1$, $\nu$ étant un diviseur impair de $n$. Ayant donc examiné tous les nombres $a^\nu \pm 1$, qui remplissent cette condition, si aucun de leurs facteurs premiers ne divise $A$, on sera assuré que les diviseurs de $A$ ne peuvent être que de la forme mentionnée $nx+1$ ou $2nx+1$; et si $n$ est impair, il faudra non-seulement que les diviseurs de $A$ soient de la forme $2nx+1$, mais qu'ils soient aussi de l'une des formes linéaires qui conviennent aux diviseurs de $t^2 \pm au^2$. Ces formes étant connues par nos Tables (au moins lorsque $a$ ne passe pas leurs limites), on pourra, par la combinaison de ces deux conditions, réduire beaucoup la multitude des nombres premiers moindres que $\sqrt{A}$ par lesquels il faut essayer de diviser $A$. Nous avons déjà donné des exemples de cette méthode dans le §. V; nous ajouterons encore les deux suivans.

(255) Considérons 1°. le nombre $2^{25}-1=(2^5-1).1082401$; et proposons-nous de trouver tous les diviseurs du facteur $1082401=A$; comme ce nombre n'est pas divisible par $2^5-1=31$, il ne peut

avoir pour diviseur que des nombres de la forme $50x+1$. De plus, le nombre $A$ étant diviseur de la formule $2^{26}-2$ qui est de la forme $t^2-2u^2$, il faudra que les diviseurs de $A$ soient de la forme $8n+1$, ou de la forme $8n+7$. Mais la forme $50x+1$ renferme les quatre

$$200x+1,\ 51,\ 101,\ 151\ ;$$

excluant donc la seconde et la troisième qui ne s'accordent pas avec les formes $8n+1$ et $8n+7$, il ne restera pour les diviseurs de $A$ que les deux formes

$$200x+1,\ 200x+151.$$

Les nombres moindres que $\sqrt{A}$ compris dans ces formes sont:

151, 201, 351, 401, 551, 601, 751, 801, 951, 1001;

d'où excluant ceux qui ne sont pas premiers, il reste les quatre seuls nombres 151, 401, 601, 751, par lesquels il faut essayer de diviser $A$.

La division ne réussit ni par 151, ni par 401, mais elle réussit par 601, et on a pour quotient 1801 ; donc le nombre $A$ n'est pas un nombre premier. Et quant au quotient 1801, il est nécessairement premier, car s'il ne l'étoit pas, il admettroit la division par un nombre moindre que $\sqrt{1801}$, ce qui n'est pas possible, puisque le moindre nombre premier qui divise $A$ est 601. Donc on a simplement $A = 601 \cdot 1801$.

Considérons 2°. le nombre $2^{27}-1 = (2^9-1) \cdot 262657$, et soit proposé de trouver les diviseurs du nombre $A = 262657$; il est facile de s'assurer que ce nombre n'est divisible par aucun de ceux qui divisent $2^3-1$ ou $2^9-1$; donc ses diviseurs, s'il en a, sont de la forme $54x+1$. D'ailleurs $A$ étant lui-même diviseur de $2^{28}-2$, les diviseurs de $A$ sont aussi de la forme $t^2-2u^2$, et par conséquent de l'une des formes $8n+1$ ou $8n+7$. Si on combine donc ces deux formes avec la forme $54x+1$, on aura les deux formes $216x+1$, $216x+55$, lesquelles ne comprennent, audessous de $\sqrt{A} = 512$, que les cinq nombres 55, 217, 271, 433, 487. Retranchant de ceux-ci les nombres composés, il ne reste à essayer que les trois nombres premiers 271, 433, 487; et comme aucun de ces trois nombres ne divise 262657, on en conclura avec certitude que 262657 est un nombre premier.

(256) En général, étant proposé un nombre quelconque $A$, on tâchera de ramener ce nombre ou un de ses multiples, à la forme $t^2+au^2$, $a$ étant un nombre le moins grand possible, et qui ne passe pas les limites des Tables. Pour cela, il faut extraire la racine quarrée tant de $A$ que de quelques-uns de ses multiples $2A$, $3A$, $4A$, &c., et on fera en sorte que le reste, positif ou négatif, soit de la forme $au^2$, $u^2$ étant le plus grand quarré par lequel ce reste est divisible.

Dès qu'on aura mis $A$, ou en général $kA$ sous la forme $t^2\pm au^2$, on sera sûr que les diviseurs de $A$ sont compris parmi les formes linéaires des diviseurs de la formule $t^2\pm au^2$, et comme ces formes linéaires excluent la moitié des nombres premiers, autant on aura trouvé de formes différentes $t^2\pm au^2$ pour $A$ ou $kA$, autant de fois on aura réduit à moitié le nombre de diviseurs à essayer pour le nombre $A$. Si donc il y a $m$ nombres premiers compris depuis 1 jusqu'à $\sqrt{A}$, et que $i$ soit le nombre des formes $t^2\pm au^2$ dont il s'agit, on n'aura plus à essayer que $(\frac{1}{2})^i.m$ nombres premiers, pour s'assurer si $A$ est premier, ou s'il ne l'est pas.

Si $A$ étoit un diviseur de la formule $a^n\pm 1$, ou $a^n\pm b^n$, $a$ et $b$ étant premiers entr'eux, on auroit de plus les conditions dont nous avons déjà parlé, qu'on combineroit avec celles qui résultent de la forme $t^2\pm au^2$.

(257) Enfin on peut encore indiquer un moyen qui le plus souvent aura du succès. Il consiste à convertir en fraction continue $\sqrt{A}$, ou $\sqrt{2A}$, $\sqrt{3A}$, &c. Car si en général $\frac{\sqrt{kA}+I}{D}$ est un quotient-complet provenant du développement de $\sqrt{kA}$, et que $\frac{p}{q}$ soit la fraction convergente qui répond à ce quotient, on aura (n°. 30) $\pm D=p^2-kAq^2$, ou $kAq^2=p^2\mp D$. Donc les diviseurs de $A$ sont diviseurs de $p^2\mp D$, ou en général de $t^2\mp Du^2$, savoir de $t^2+Du^2$ lorsque le quotient-complet est de rang pair, et de $t^2-Du^2$ lorsqu'il est de rang impair.

Dans cette opération, le nombre $D$ n'excède jamais $2\sqrt{kA}$, et le plus souvent il est beaucoup plus petit; ainsi on pourra

connoître, par ce moyen, des formules assez simples $t^2 \pm Du^2$ dont les facteurs de $A$ doivent être diviseurs. Et s'il arrivoit qu'on trouvât deux formules $t^2+Du^2$, $t^2-Du^2$ contenant la même valeur de $D$, il s'ensuivroit que $A$ qui divise l'une et l'autre, divise $t^2+t'^2$, et par conséquent, que ses propres diviseurs doivent être aussi de la forme $y^2+z^2$, et de la forme linéaire $4x+1$, ce qui abrégeroit les calculs.

(258) Appliquons ces principes au nombre $333667=A$. On trouvera d'abord, par l'extraction de la racine, $A=577^2+82.3^2$; donc $A$ est de la forme $t^2+82u^2$, et ses diviseurs doivent être du nombre de ceux qui conviennent à cette formule. Pour trouver d'autres formes, j'essaye de décomposer des multiples de $A$, je trouve par exemple $3A=1001001=(1001)^2-10(10)^2$, quantité de la forme $t^2-10u^2$; donc les diviseurs de $A$ doivent être de l'une des formes qui conviennent aux diviseurs de $t^2-10u^2$. Ces deux formes réduiroient déjà au quart seulement les nombres premiers qui sont à essayer pour diviseurs de $A$, et qui doivent être moindres que $\sqrt{A}$ ou 577. Mais comme l'opération seroit encore longue, nous chercherons de nouvelles formes par le développement de $\sqrt{A}$ en fraction continue. Ce développement donne les quotiens-complets qui suivent :

$$\frac{\sqrt{A}+0}{1},\ \frac{\sqrt{A}+577}{738},\ \frac{\sqrt{A}+161}{417},\ \frac{\sqrt{A}+256}{643},\ \frac{\sqrt{A}+387}{286},$$
$$\frac{\sqrt{A}+471}{391},\ \frac{\sqrt{A}+311}{606},\ \frac{\sqrt{A}+295}{407},\ \frac{\sqrt{A}+519}{158},\ \frac{\sqrt{A}+429}{947},$$
$$\frac{\sqrt{A}+518}{69},\ \frac{\sqrt{A}+517}{962},\ \frac{\sqrt{A}+445}{141},\ \frac{\sqrt{A}+542}{288},\ \&c.$$

De-là on voit que les diviseurs de $A$ doivent diviser les formules

$$t^2+738u^2 \text{ ou } t^2+82u^2,\ t^2-417u^2,\ t^2+643u^2,\ \&c.$$

Les plus simples sont $t^2+82u^2$, $t^2-69u^2$, et $t^2+2u^2$, car c'est à cette dernière que se réduit la formule $t^2+288u^2$ donnée immédiatement par le terme $D=288$.

Si à ces formes on ajoute celle qui a été déjà trouvée $t^2-10u^2$, on sera en état de diminuer beaucoup le nombre des essais qui

restent à faire. Et d'abord les diviseurs de $t^2+2u^2$ étant de la forme $8n+1$ ou $8n+3$; et ceux de $t^2-10u^2$ étant $40x+1$, 3, 9, 13, 27, 31, 37, 39 : si on rejette parmi ceux-ci les formes qui ne sont pas $8n+1$ ou $8n+3$, il ne restera que les formes $40x+1$, 3, 9, 27.

Maintenant si on développe tous les nombres premiers compris dans ces formes jusqu'à 577 qui est $\sqrt{A}$, on trouvera

1, 3, 41, 43, 67, 83, 89, 107, 163, 227, 241, 281, 283,

347, 401, 409, 443, 449, 467, 481, 521, 523, 547, 563, 569.

Éliminant parmi ceux-ci ceux qui ne peuvent être diviseurs de $t^2-69u^2$, ce qu'on reconnoîtra facilement (Table III) par les formes $276x+a$ qui conviennent à ces diviseurs, il restera

1, 83, 89, 107, 163, 227, 281, 401, 409, 467, 521,

547, 563, 569.

Enfin rejetant de même parmi ces derniers ceux qui ne peuvent être diviseurs de la formule $t^2+82u^2$, ou qui ne sont pas de la forme $328x+a$ qui convient à ces diviseurs (Table VI), il ne restera à essayer que les sept nombres premiers

83, 107, 163, 401, 409, 467, 569.

Or aucun de ces nombres ne divise 333667, ainsi on est assuré que 333667 est un nombre premier.

On auroit diminué beaucoup le nombre des tentatives, si on eût observé que $3A$ étant $1001001 = 10^6+10^3+1 = \frac{10^9-1}{10^3-1}$, les diviseurs de $A$ doivent diviser $10^9-1$, et par conséquent doivent avoir la forme $18x+1$. Mais nous avons voulu faire voir comment on doit procéder lorsqu'on n'a aucune donnée sur la nature du nombre qu'on examine.

(259) Proposons-nous encore le nombre $10\,091\,401 = A$ : il faudroit, suivant le principe général, essayer la division par tous les nombres premiers moindres que $\sqrt{A}$, c'est-à-dire moindres que 3176. Mais pour diminuer le nombre de ces tentatives, nous

chercherons tout d'un coup, par le développement de $\sqrt{A}$ en fraction continue, les diverses formules $t^2 \pm D u^2$ dont $A$ doit être diviseur. Soit $\frac{\sqrt{A} + I}{D}$ l'expression générale du quotient-complet, on trouvera que les valeurs de $D$ fournies par cette opération sont successivement

$D=1$, $4425=177.5^2$, $1928=482.2^2$, $1709$, $2189$, $3033=337.3^2$, $2872=718.2^2$, $2511=31.9^2$, $3755$, $384=6.8^2$, $5585$, $437$, $3648=57.8^2$, $2619$, $2495$, $183$, $2019$, $720=5.12^2$, $2963$, $152=38.2^2$, $2061=229.3^2$, $365$, $480=30.4^2$, $1119$, $3415$, $2712=678.2^2$, $2525=101.5^2$, $3789=421.3^2$, $184=46.2^2$, &c.

De-là on déduit déjà plusieurs formules assez simples, desquelles $A$ doit être diviseur. Ces formules sont :

$t^2+31u^2$, $t^2+6u^2$, $t^2-57u^2$, $t^2+5u^2$, $t^2+38u^2$, $t^2-30u^2$, $t^2-46u^2$.

Mais il est à observer que la formule $t^2-30u^2$ n'apprend rien de plus que les deux précédentes $t^2+6u^2$, $t^2+5u^2$; car si un nombre premier est diviseur de $t^2+6u^2$ et de $t^2+5u^2$, il sera diviseur de $t^2-30u^2$; de même la formule $t^2+38u^2$ est censée comprise dans les deux précédentes $t^2+6u^2$, $t^2-57u^2$. Il ne reste par conséquent des sept formules précédentes, que cinq qui soient distinctes les unes des autres, et qui pouvant chacune réduire le nombre des essais à moitié, pourront par leur combinaison réduire ce nombre à sa trente-deuxième partie. Par ce moyen, le nombre des essais, ou celui des nombres premiers moindres que $\sqrt{A}$, qui auroit été environ 454, se réduit à 14, et l'opération devient praticable. On auroit pu encore prolonger davantage le calcul des valeurs de $D$, et il en seroit résulté les nouvelles formules $t^2-55u^2$, $t^2-97u^2$, $t^2+3u^2$, dont $A$ doit être diviseur. Avec tous ces secours, voici comment on trouvera les formes linéaires qui conviennent aux diviseurs de $A$.

1°. Les diviseurs de $t^2+3u^2$ sont en général de la forme $6x+1$, laquelle contient les quatre formes $24x+1$, 7, 13, 19.

2°. De ces quatre formes, il n'y en a que deux qui peuvent diviser $t^2+6u^2$, ce sont $24x+1$, $24x+7$.

3°. Ces dernières, considérées par rapport aux multiples de 5, contiennent les huit formes $120x+1$, 7, 31, 49, 73, 79, 97, 103, parmi lesquelles écartant celles qui ne peuvent diviser $t^2+5u^2$, il restera les quatre formes

$$120x+1,\ 7,\ 49,\ 103.$$

Les nombres premiers contenus dans ces formes diviseront donc à-la-fois les trois formules $t^2+3u^2$, $t^2+6u^2$, $t^2+5u^2$.

4°. Si les quatre formes précédentes sont développées par rapport aux multiples de 11; c'est-à-dire, si au lieu de $x$, on met successivement $11x$, $11x+1$, $11x+2$, &c., et qu'on rejette les multiples de 11, il en résulte les quarante formes suivantes :

$1320x+1$, 7, 49, 103, 127, 169, 223, 241, 247, 289,
343, 361, 367, 409, 463, 481, 487, 529, 601, 607,
703, 721, 727, 769, 823, 841, 889, 943, 961, 967,
1009, 1063, 1081, 1087, 1129, 1183, 1201, 1207, 1249, 1303.

Parmi ces formes, il ne faut conserver que celles qui peuvent diviser $t^2-55u^2$; pour cet effet, on prendra dans la Table III les formes $220x+a$ qui divisent $t^2-55u^2$; et la comparaison faite, on trouvera qu'il ne reste que les vingt formes :

$1320x+1$, 49, 103, 169, 223; 247, 289, 361, 367, 463;
487, 529, 727, 823, 841; 889, 961, 1081, 1087, 1303.

Maintenant si l'on prend les nombres moindres que 3176 compris dans cette formule, et qu'on en exclue les nombres composés, ils se réduiront aux suivans :

103, 223, 367, 487, 727, 823, 1087, 1321, 1423, 1489
1543, 1609, 1783, 2143, 2161, 2281, 2689, 3001, 3169.

Excluant encore de ceux-ci les nombres qui ne peuvent diviser $t^2+31u^2$, il restera les onze suivans :

103, 727, 1087, 1321, 1423, 1489, 1609, 1783,
2143, 2281, 3169.

Enfin si on exclut de même ceux qui ne peuvent diviser $t^2+38u^2$, on n'aura plus que les six nombres

727, 1087, 1423, 1489, 1783, 2281;

et la condition qu'ils soient diviseurs de $t^2 - 46u^2$, les réduira de nouveau aux trois nombres

727, 1423, 2281.

Il est inutile d'aller plus loin dans la réduction de ces nombres, et on auroit pu même se dispenser d'aller aussi loin; or on trouve qu'aucun de ces nombres ne divise 10 091 401, on pourra donc conclure, avec certitude, que 10 091 401 est un nombre premier.

Euler est parvenu au même résultat, en s'assurant que 10091 401 ne peut se décomposer que d'une seule manière en deux quarrés, ce qui est un caractère essentiel des nombres premiers $4n+1$. (Voyez le Tom. IX des *Novi Comm. Petrop.* Voyez aussi les Mémoires de Berlin, année 1771.)

---

TROISIEME

# TROISIÈME PARTIE.

## *THÉORIE DES NOMBRES CONSIDÉRÉS COMME DÉCOMPOSABLES EN TROIS QUARRÉS.*

### §. I. *Définition de la forme trinaire. Nombres et diviseurs quadratiques auxquels cette forme ne peut convenir.*

(260) Nous appellerons, pour abréger, *forme trinaire* d'un nombre, toute manière d'exprimer ce nombre par la somme de trois quarrés. Ainsi 59 pouvant se représenter par $25+25+9$, et par $49+9+1$, chacune de ces expressions sera une forme trinaire de 59.

Une forme trinaire est composée en général de trois quarrés, mais elle peut ne l'être que de deux ou même que d'un seul, parce que, dans ces cas, zéro sera regardé comme quarré complétif. On peut donc dire que 45 est susceptible de deux formes trinaires, savoir $36+9$ et $25+16+4$; de même le nombre 9 en comporte deux, qui sont 9 et $4+4+1$.

Lorsqu'un nombre est divisible par un quarré, la forme trinaire qui convient particulièrement à ce nombre, est celle dont les trois termes ne sont pas divisibles par un même quarré. Ainsi 45 a pour forme trinaire propre $25+16+4$; l'autre forme $36+9$, ou $9(4+1)$, dépendante du facteur 5, est en quelque sorte étrangère au nombre 45. De même la forme trinaire caractéristique de 9 est $4+4+1$, celle de 25 est $16+9$, ou $16+9+0$ (dont les trois termes ne sont pas divisibles par un même nombre), et ainsi des autres.

(261) *Aucun nombre* $8n+7$, *ni le produit d'un tel nombre par une puissance paire de* 2, *ne peut être de forme trinaire.*

Car tout quarré pair étant représenté par $4m$, et tout quarré

impair par $8n+1$, la somme de trois quarrés, si elle est impaire, ne peut être que de l'une des deux formes

$$8p+1+8q+1+8r+1=8k+3$$
$$4p+4q+8r+1=4k+1,$$

lesquelles ne renferment pas la forme $8n+7$; et la somme de trois quarrés, si elle est paire, ne peut être que le produit d'une puissance paire de 2 par un nombre de l'une des trois formes

$$8p+1+8q+1+8r+1=8k+3$$
$$8p+1+8q+1+4r=4k+2$$
$$8p+1+4q+4r=4k+1.$$

Donc jamais la somme de trois quarrés n'est de la forme $(8n+7)2^{2i}$; encore moins les nombres de cette forme peuvent-ils être composés de un ou de deux quarrés seulement.

Quant aux nombres qui ne sont pas de la forme $(8n+7)2^{2i}$, non-seulement on ne voit rien qui empêche qu'ils soient composés de trois quarrés, mais on s'assurera par l'expérience qu'ils sont composés ainsi, et qu'en conséquence ils sont tous de forme trinaire.

(262) On trouvera également que parmi les diviseurs quadratiques d'une même formule $t^2+cu^2$, où $c$ n'est pas de la forme $(8n+7)2^{2i}$, il y en a toujours un ou plusieurs qu'on peut décomposer actuellement en trois quarrés; de sorte qu'alors le diviseur $py^2+2qyz+rz^2$ pourra être mis sous la forme

$$(my+nz)^2+(m'y+n'z)^2+(m''y+n''z)^2.$$

Cette décomposition, qui a lieu indéfiniment pour toutes valeurs des indéterminées $y$ et $z$, fournit un caractère particulier de ce genre de diviseurs : nous appellerons *diviseurs quadratiques trinaires*, ou simplement *diviseurs trinaires*, ceux qui jouissent de cette propriété.

Par exemple, la formule $t^2+65u^2$ a un diviseur quadratique trinaire, lequel est

$$9y^2+10yz+10z^2=(2y+3z)^2+4y^2+(y-z)^2.$$

La même formule a un autre diviseur quadratique $4n+1$, qui est $18y^2+10yz+5z^2$, mais celui-ci n'est pas de forme trinaire; car on tenteroit inutilement de le décomposer en trois quarrés comme le précédent.

(263) Nous observerons qu'il est certaines classes de diviseurs quadratiques qui ne peuvent jamais être de forme trinaire.

1°. Lorsque $c$ est de la forme $4n+1$, les diviseurs quadratiques de la formule $t^2+cu^2$ sont de deux sortes, l'une contenant les nombres $4n+1$, l'autre contenant les nombres $4n-1$. Ceux-ci renferment indistinctement les diviseurs $8n+3$, $8n+7$, et comme aucun nombre $8n+7$ n'est la somme de trois quarrés, il s'ensuit qu'aucun diviseur quadratique $4n-1$, ne sauroit être de forme trinaire.

2°. Lorsque $c$ est de la forme $8n+7$, il n'y a absolument aucun diviseur quadratique de la formule $t^2+cu^2$ qui puisse être de forme trinaire. La raison en est que chaque diviseur quadratique contient indistinctement les diviseurs $4n+1$ et $4n-1$; il contient donc aussi les diviseurs $8n+7$ dont aucun n'est décomposable en trois quarrés; donc le diviseur quadratique en général ne peut être de forme trinaire.

3°. Lorsque $c$ est de la forme $8n+3$, il ne peut non plus y avoir aucun diviseur quadratique de forme trinaire, par la même raison qui vient d'être apportée. Cependant il pourra arriver que le double d'un diviseur quadratique soit de forme trinaire. Par exemple, $y^2+yz+5z^2$ représente tout diviseur impair de la formule $t^2+19z^2$; ce diviseur considéré ainsi en général, n'est point décomposable en trois quarrés, mais son double $2y^2+2yz+10z^2$ se résout en ces trois quarrés $y^2+9z^2+(y+z)^2$.

4°. Étant proposée la formule $t^2+2au^2$, dans laquelle $a$ est de la forme $4n+1$, les diviseurs quadratiques de cette formule sont de deux sortes; les uns contenant les nombres $8n+5$, $8n+7$, les autres contenant les nombres $8n+1$, $8n+3$. Il n'y a donc que ceux-ci qui puissent être de forme trinaire.

5°. Enfin lorsque $a$ est de la forme $4n-1$, les diviseurs quadratiques de la formule $t^2+2au^2$ sont de deux sortes, les uns contenant les nombres $8n+1$, $8n+7$; les autres contenant les nombres $8n+3$, $8n+5$. Il est évident que c'est seulement parmi ces derniers que peuvent se trouver les diviseurs de forme trinaire.

(264) Étant donnée une forme trinaire $a^2+b^2+c^2$ du nombre $A$, on pourra le plus souvent trouver, par son moyen, une ou plusieurs autres formes trinaires du même nombre.

Car 1°. si des trois quarrés donnés il en est deux dont la somme $a^2+b^2$ ne soit pas un nombre premier, ou le double d'un premier, cette somme pourra se changer (n°. 236) en une somme semblable $f^2+g^2$; de sorte qu'on aura $A=f^2+g^2+c^2$.

2°. Si l'on fait $\frac{a+b+c}{3}=m$, on aura en général

$$A=a^2+b^2+c^2=(2m-a)^2+(2m-b)^2+(2m-c)^2;$$

et comme on peut prendre à volonté les signes de $a$, $b$, $c$, on pourra presque toujours faire en sorte que $m$ soit entier, ce qui donnera une seconde forme trinaire du nombre $A$. Il faut cependant excepter le cas où deux des trois nombres $a$, $b$, $c$ seroient divisibles par 3, et le troisième non-divisible, car alors $m$ ne pourroit être un entier.

Il faut aussi excepter le cas où l'un des trois nombres $a$, $b$, $c$ seroit égal à la demi-somme des deux autres. Car si l'on a, par exemple, $b+c=2a$, cette relation particulière donnera $m=a$, et alors la forme $(2m-a)^2+(2m-b)^2+(2m-c)^2$ sera identique avec la forme donnée $a^2+b^2+c^2$.

(265) Pour donner un exemple de ces transformations, soit le nombre $89=9^2+2^2+2^2$; en faisant $a=9$, $b=2$, $c=-2$, on aura $m=\frac{a+b+c}{3}=3$, et par conséquent $(2m-a)^2+(2m-b)^2+(2m-2)^2=3^2+4^2+8^2$, seconde forme trinaire de 89. Celle-ci fournira semblablement une troisième forme $7^2+6^2+2^2$, puis la troisième une quatrième $5^2+0^2+8^2$. On trouve donc par ce moyen les quatre formes trinaires dont 89 est susceptible.

La même transformation pourra quelquefois être appliquée à des formules quadratiques indéfinies. Si l'on a, par exemple, la formule $(4y+z)^2+(y-z)^2+4z^2$, et qu'on fasse $a=4y+z$, $b=-y+z$, $c=-2z$, on aura $m=\frac{a+b+c}{3}=y$, et la forme trinaire proposée sera changée en cette autre forme :

$$(2y+z)^2+(3y-z)^2+(2y+2z)^2.$$

## §. II. *Théorèmes relatifs aux diviseurs trinaires.*

(266) Théorème I. Soit c *un nombre impair ou double d'un impair, composé des trois quarrés* $f^2+g^2\mu^2+g^2\nu^2$, *où* $\mu$ *et* $\nu$ *sont premiers entr'eux, je dis que le nombre* $\mu^2+\nu^2$ *sera diviseur de* $t^2+cu^2$.

*Réciproquement si l'on a* $c=f^2+\pi g^2$, *et que* $\pi$ *soit diviseur de* $t^2+cu^2$, *et en même temps premier à* c, *je dis que* $\pi$ *sera la somme de deux quarrés premiers entr'eux.*

Car 1°. en faisant $\mu^2+\nu^2=\pi$, les diviseurs premiers de $\pi$ ne sauroient être que des nombres premiers $4n+1$ ou 2. Soit $\omega$ un de ces diviseurs, puisqu'on a $\pi g^2=c-f^2$, $\omega$ sera diviseur de $c-f^2$, et par conséquent il le sera aussi de $x^2+c$ (n°. 171). Mais si chaque diviseur de $\pi$ est diviseur de la formule $t^2+cu^2$, il s'ensuit que le nombre $\pi$ lui-même est diviseur de $t^2+cu^2$.

2°. Si on suppose que $\pi$ est diviseur de $t^2+cu^2$, et qu'on ait $c=f^2+\pi g^2$, il faudra que $\pi$ divise $t^2+f^2u^2+\pi g^2u^2$, ou simplement $t^2+f^2u^2$. Mais $t$ et $u$ sont premiers entr'eux. Quant à $t$ et $f$, s'ils avoient un commun diviseur $\alpha$, ce nombre $\alpha$ ne pourroit diviser $\pi$, sans quoi il diviseroit $c$, et ainsi $c$ et $\pi$ ne seroient plus premiers entr'eux, comme on le suppose. Donc en faisant $t=\alpha t'$, $f=\alpha f'$, ce qui donne $t^2+f^2u^2=\alpha^2(t'^2+f'^2u^2)$, les nombres $t'$ et $f'u$ seront premiers entr'eux; et comme $\pi$ n'a point de diviseur commun avec $\alpha$, il faudra que $\pi$ divise la somme des deux quarrés premiers entr'eux $t'^2+f'^2u^2$; donc $\pi$ sera une somme semblable $\mu^2+\nu^2$, ce qui est la seconde partie du théorême.

*Corollaire.* Si le nombre $c$ est de la forme $f^2\mu^2\nu^2+g^2\nu^2\lambda^2+h^2\lambda^2\mu^2$, dans laquelle les termes pris deux à deux ont pour communs diviseurs $\lambda^2, \mu^2, \nu^2$, il suit de la première partie du théorême, que les trois nombres $f^2\mu^2+g^2\lambda^2$, $g^2\nu^2+h^2\mu^2$, $h^2\lambda^2+f^2\nu^2$, composés chacun de deux quarrés premiers entr'eux, seront diviseurs de la formule $t^2+cu^2$. On verra de plus, n°. 274, qu'ils appartiennent tous trois à un même diviseur quadratique.

(267) THÉORÈME II. *Soit* c *un nombre premier ou le double d'un tel nombre, et supposons qu'on ait à-la-fois* $c = f^2 + \pi g^2 = f'^2 + \pi' g'^2$ ; *si les nombres* $\pi$ *et* $\pi'$ *sont diviseurs de* $t^2 + cu^2$, *je dis qu'ils ne pourront appartenir à un même diviseur quadratique, à moins qu'on n'ait* $\pi = \mu^2 + \nu^2$, $\pi' = \mu'^2 + \nu'^2$, *et que les trois quarrés* $f^2 + \mu^2 g^2 + \nu^2 g^2$ *ne soient les mêmes, à l'ordre près, que les trois quarrés* $f'^2 + \mu'^2 g'^2 + \nu'^2 g'^2$.

En effet, si les nombres $\pi$ et $\pi'$ appartiennent à un même diviseur quadratique, il faudra qu'on ait (n°. 231)

$$\pi\pi' = y^2 + cz^2.$$

Cette valeur étant substituée dans le produit des deux valeurs de $c$, on aura

$$c^2 = f^2 f'^2 + \pi(f'^2 g^2 + f^2 g'^2) + g^2 g'^2 (y^2 + cz^2);$$

d'où l'on conclut d'abord que chacun des termes $ff'$, $gg'y$ est moindre que $c$. On aura ensuite $(c - f^2)(c - f'^2) = \pi\pi' g^2 g'^2 = g^2 g'^2 (y^2 + cz^2)$, ou

$$\frac{f^2 f'^2 - g^2 g'^2 y^2}{c} = g^2 g'^2 z^2 + f^2 + f'^2 - c, \qquad (1)$$

il faut donc que le premier membre se réduise à un entier. Cela posé, nous examinerons successivement les deux cas mentionnés dans le théorême.

*Premier cas.* Si $c$ est un nombre premier, il faudra que $ff' + gg'y$ ou $ff' - gg'y$ soit divisible par $c$. Mais on a déjà vu que chacun des termes $ff'$, $gg'y$ est moindre que $c$, ainsi l'on ne peut faire que l'une ou l'autre des deux suppositions suivantes :

$$ff' + gg'y = c$$
$$ff' - gg'y = 0.$$

La première donneroit

$$\frac{f^2 f'^2 - g^2 g'^2 y^2}{c} = 2ff' - c = g^2 g'^2 z^2 + f^2 + f'^2 - c,$$

ou $(f - f')^2 + g^2 g'^2 z^2 = 0$, ce qui est impossible. La seconde supposition donne

$$c = f^2 + f'^2 + g^2 g'^2 z^2.$$

Comparant cette valeur avec les deux supposées $c = f^2 + \pi g^2$, $c = f'^2 + \pi' g'^2$, on en tire

$$\pi g^2 = f'^2 + g^2 g'^2 z^2$$
$$\pi' g'^2 = f^2 + g^2 g'^2 z^2,$$

ce qui prouve que $\frac{f'}{g}$ et $\frac{f}{g'}$ doivent être des entiers. Soit donc $f'=g\theta$, $f=g'\theta'$, on aura

$$\pi=\theta^2+g'^2z^2$$
$$\pi'=\theta'^2+g^2z^2;$$

valeurs telles que le développement des deux quantités $f^2+\pi g^2$, $f'^2+\pi' g'^2$ donne les trois mêmes quarrés ou la même forme trinaire

$$c=g^2\theta^2+g'^2\theta'^2+g^2g'^2z^2.$$

D'où l'on voit 1°. que les nombres $\pi$ et $\pi'$ sont chacun la somme de deux quarrés conformément au théorème I; 2°. que les trois quarrés résultans de la forme $f^2+\pi g^2$ sont identiques avec les trois quarrés résultans de la forme $f'^2+\pi' g'^2$.

*Second cas.* Si l'on a $c=2a$, $a$ étant un nombre premier, il faudra que l'un des facteurs $ff'+gg'y$, $ff'-gg'y$ soit divisible par $a$; et comme on a toujours $ff'+gg'y<2c$ ou $<4a$, on ne pourra faire que les deux suppositions suivantes, $k$ étant $<4$:

$$ff'+gg'y=ka$$
$$ff'-gg'y=ka.$$

Ces deux équations reviennent à la même, parce qu'on peut supposer $y$ positif ou négatif; ainsi il suffira d'en examiner une. Or la seconde donne $f^2f'^2-g^2g'^2y^2=2ff'ka-k^2a^2$, quantité qui, d'après l'équation (1), doit être divisible par $c$ ou par $2a$. De-là on voit que $k$ doit être pair, et qu'ainsi il faut faire $k=2$ ou $k=0$. Mais alors on retombe sur les deux suppositions $ff'-gg'y=2a=c$, $ff'-gg'y=0$, les mêmes auxquelles on a été conduit dans le développement du premier cas. On en tirera donc encore la même conclusion conforme à l'énoncé du théorème.

(268) THÉORÈME III. *Si un diviseur quadratique de la formule* $t^2+cu^2$ *est décomposable en trois quarrés, tels que* $(my+nz)^2+(m'y+n'z)^2+(m''y+n''z)^2$, *je dis que cette forme trinaire du diviseur en fournira une correspondante du nombre* $c$, *laquelle sera* $c=(mn'-m'n)^2+(m'n''-m''n')^2+(m''n-mn'')^2$.

Car en représentant le diviseur dont il s'agit par la formule ordinaire $py^2+2qyz+rz^2$, on aura

$$p = m^2 + m'^2 + m''^2$$
$$q = mn + m'n' + m''n''$$
$$r = n^2 + n'^2 + n''^2.$$

Or ces valeurs étant substituées dans l'équation $c = pr - q^2$, on en tire

$$c = (mn' - m'n)^2 + (m'n'' - m''n')^2 + (m''n - mn'')^2.$$

Donc il y a toujours une forme trinaire déterminée de $c$ qui correspond à une forme trinaire déterminée du diviseur quadratique $py^2 + 2qyz + rz^2$.

(269) *Remarque I.* Lorsque $c$ est de la forme $8k+3$, au lieu du diviseur quadratique à coefficiens impairs, lequel ne pourroit jamais être de forme trinaire, on considérera son double $2py^2 + 2qyz + 2rz^2$ où l'on a $4pr - q^2 = c$. Si donc ce double diviseur impair, ou ce diviseur $4n+2$, est décomposable en trois quarrés, il y aura toujours une valeur correspondante de $c$ exprimée aussi par la somme de trois quarrés déterminés, c'est-à-dire en d'autres termes que chaque forme trinaire du diviseur quadratique $4n+2$ en fournit une correspondante du nombre $c$. Et celle-ci est toujours composée de trois quarrés impairs, car il n'y a aucune autre supposition qui puisse donner une somme $8k+3$.

*Remarque II.* La décomposition d'un diviseur quadratique ou de son double en trois quarrés, ne sauroit avoir lieu lorsque $c = 8k+7$; car si cette décomposition étoit possible, il résulteroit du théorême précédent, que $c$ est la somme de trois quarrés; ce qui est impossible à l'égard de tout nombre $8k+7$.

*Remarque III.* Les trois quarrés trouvés en général pour la valeur de $c$ se réduisent à deux ou même à un seul dans des cas qu'il est facile de prévoir.

1°. Pour qu'on ait $m''n' - m'n'' = 0$, ou $\frac{m''}{n''} = \frac{m'}{n'}$, il faut que le quarré $(m''y + n''z)^2$ ait un rapport constant avec le quarré $(m'y + n'z)^2$; et réciproquement, si le diviseur quadratique $\Delta$ est de la forme

$$\Delta = (my + nz)^2 + \alpha^2(My + Nz)^2 + \mathcal{C}^2(My + Nz)^2,$$

la

la valeur correspondante de $c$ ne contiendra que deux quarrés, et sera

$$c=\alpha^2(mN-nM)^2+\zeta^2(mN-nM)^2.$$

De plus, ces deux quarrés seront affectés d'un commun diviseur $(mN-nM)^2$, ou s'il n'y a pas de commun diviseur, il faudra supposer $mN-nM=\pm 1$. Mais alors si l'on fait $my+nz=y'$, $My+Nz=z'$, on ne nuit en rien à la généralité des valeurs de $y$ et $z$ (n°. 45), et le diviseur devient $y'^2+(\alpha^2+\zeta^2)z'^2$ ou $y'^2+cz'^2$. Donc lorsque $c$ n'a point de facteur quarré, et qu'on n'a point $c=\alpha^2+\zeta^2$, le cas que nous venons de développer ne pourra avoir lieu, et il faudra que tout diviseur trinaire de la formule $t^2+cu^2$, donne une forme trinaire de $c$ composée de trois quarrés dont aucun ne pourra être nul.

2°. Pour que les trois quarrés qui composent la valeur de $c$ se réduisent à un seul, il faut qu'on ait à-la-fois $m'n''-m''n'=0$, $m''n-mn''=0$, ce qui donne $m''=0$, $n''=0$. Donc alors le diviseur quadratique dont il s'agit seroit $(my+nz)^2+(m'y+n'z)^2$, et le nombre correspondant $c=(mn'-m'n)^2$.

(270) Théorème IV. *Réciproquement étant donnée une forme trinaire du nombre* c, *on pourra toujours trouver un diviseur quadratique de la formule* $t^2+cu^2$, *lequel répondra à la valeur donnée de* c *et sera également de forme trinaire.*

Soit la forme trinaire donnée $c=F^2+(G^2+H^2)\theta^2$, où l'on pourra supposer $G$ et $H$ premiers entr'eux; si on détermine $\zeta$ et $\alpha$ d'après l'équation $F=G\zeta-H\alpha$, le diviseur quadratique correspondant à la valeur de $c$ sera

$$\Delta=(Gy+\alpha z)^2+(Hy+\zeta z)^2+\theta^2z^2.$$

En effet, si on compare cette quantité à la formule $(my+nz)^2+(m'y+n'z)^2+(m''y+n''z)^2$, et qu'ensuite on substitue les valeurs de $m, n, m', n'$, &c. dans la formule $c=(mn'-m'n)^2+(m'n''-m''n')^2+(m''n-mn'')^2$, on en déduira

$$c=(G\zeta-H\alpha)^2+H^2\theta^2+G^2\theta^2=F^2+(G^2+H^2)\theta^2;$$

ce qui est la forme trinaire donnée.

Donc toute valeur trinaire du nombre $c$ fournit un diviseur quadratique qui répond à cette valeur, et qui est lui-même de forme

trinaire. Ce diviseur se réduit à la forme ordinaire $py^2+2qyz+rz^2$ en prenant

$$p=G^2+H^2$$
$$q=G\alpha+H\zeta$$
$$r=\alpha^2+\zeta^2+\theta^2.$$

Pour faire une application de ces formules, soit la valeur donnée $256+49+16=321=c$, on fera $F=16$, $G=7$, $H=4$, $\theta=1$, et d'abord il faudra résoudre l'équation $16=7\zeta-4\alpha$, laquelle donne $\zeta=4$, $\alpha=3$. Donc le diviseur quadratique qui répond à la forme donnée est $(7y+3z)^2+(4y+4z)^2+z^2$. Ce diviseur se simplifie, en mettant $z-y$ à la place de $z$, et il devient $(4y+3z)^2+(4z)^2+(z-y)^2=17y^2+22yz+26z^2$.

Prenons pour second exemple le nombre $331=c$, et sa forme trinaire $25+81+225$; celle-ci étant comparée terme à terme à la forme générale $F^2+(G^2+H^2)\theta^2$, on aura $F=5$, $G=3$, $H=5$, $\theta=3$; résolvant ensuite l'équation $5=3\zeta-5\alpha$, on en tire $\zeta=0$, $\alpha=-1$. Donc le diviseur cherché $\Delta=(3y-z)^2+25y^2+9z^2=34y^2-6yz+10z^2$. Dans ce cas, ainsi que dans tous ceux où $c$ est de forme $8n+3$, on trouve pour résultat le double d'un diviseur quadratique impair; car c'est ce double, et non le diviseur simple, qui peut être de forme trinaire (263).

La démonstration que nous venons de donner, prouve qu'il existe toujours, à l'égard de la formule $t^2+cu^2$, un diviseur quadratique correspondant à une forme trinaire donnée du nombre $c$; mais comme cette proposition est la base d'une théorie importante, il est nécessaire de rechercher par une analyse directe et rigoureuse, s'il n'y a qu'un de ces diviseurs, ou s'il peut y en avoir plusieurs. Cet objet, et quelques autres accessoires, seront traités dans le §. suivant.

## §. III. *Méthode directe pour trouver le diviseur trinaire de la formule* $t^2+cu^2$, *correspondant à une valeur trinaire donnée du nombre* c.

(271) Nous supposerons d'abord que la valeur trinaire donnée $c=A^2+B^2+C^2$ est telle, que les trois quarrés $A^2$, $B^2$, $C^2$ ne sont pas divisibles par un même facteur. Ces quarrés pourront néanmoins, pris deux à deux, avoir des diviseurs communs; c'est pourquoi si on appelle $\lambda$ le plus grand commun diviseur de $B$ et $C$, $\mu$ celui de $A$ et $C$, et $\nu$ celui de $A$ et $B$, la valeur trinaire donnée $A^2+B^2+C^2$ prendra la forme $f^2\mu^2\nu^2+g^2\nu^2\lambda^2+h^2\lambda^2\mu^2$, où l'on doit regarder comme premiers entr'eux $f\mu$ et $g\lambda$, $f\nu$ et $h\lambda$, $g\nu$ et $h\mu$.

Soit $\Delta$ un diviseur trinaire quelconque de la formule $t^2+cu^2$, en sorte qu'on ait

$$\Delta=(My+Nz)^2+(M'y+N'z)^2+(M''y+N''z)^2;$$

la valeur correspondante de $c$ sera

$$c=(MN'-M'N)^2+(M'N''-M''N')^2+(M''N-MN'')^2.$$

Et pour que cette forme trinaire coincide avec la valeur donnée de $c$, il faudra qu'on ait

$$MN'-M'N=h\lambda\mu$$
$$M'N''-M''N'=f\mu\nu$$
$$M''N-MN''=g\nu\lambda.$$

Ces trois équations doivent servir à trouver les valeurs des coefficiens $M$, $N$, $M'$, &c., en laissant toutefois l'indétermination qui convient à la nature des diviseurs quadratiques. Elles donnent d'abord par leur combinaison, les deux suivantes qui sont linéaires:

$$f\mu\nu\, M+g\nu\lambda\, M'+h\lambda\mu\, M''=0$$
$$f\mu\nu\, N+g\nu\lambda\, N'+h\lambda\mu\, N''=0;$$

ou, ce qui revient au même,

$$f.\frac{M}{\lambda}+g.\frac{M'}{\mu}+h.\frac{M''}{\nu}=0$$
$$f.\frac{N}{\lambda}+g.\frac{N'}{\mu}+h.\frac{N''}{\nu}=0.$$

Mais on a déjà observé que $\lambda$ ne doit avoir aucun diviseur commun avec $\mu$ ni avec $\nu$, donc le terme $f\frac{M}{\lambda}$ doit se réduire à un entier; et puisqu'en même temps $f$ et $\lambda$ sont premiers entr'eux, il faut que $\frac{M}{\lambda}$ soit un entier. On prouvera de même que les cinq autres quantités $\frac{M'}{\mu}$, $\frac{M''}{\nu}$, $\frac{N}{\lambda}$, $\frac{N'}{\mu}$, $\frac{N''}{\nu}$, doivent être des entiers; soit donc

$$M = \lambda m,\ M' = \mu m',\ N'' = \nu m''$$
$$N = \lambda n,\ N' = \mu n',\ N'' = \nu n'';$$

et le diviseur quadratique qui répond à la forme trinaire donnée deviendra

$$\Delta = \lambda^2 (my + nz)^2 + \mu^2 (m'y + n'z)^2 + \nu^2 (m''y + n''z)^2;$$

d'où l'on voit que les trois termes de ce diviseur sont divisibles respectivement par les mêmes quarrés $\lambda^2$, $\mu^2$, $\nu^2$, qui divisent deux à deux les termes de la valeur trinaire donnée $f^2\mu^2\nu^2 + g^2\nu^2\lambda^2 + h^2\lambda^2\mu^2$.

(272) Maintenant pour déterminer les nouveaux coefficiens $m$, $n$, $m'$, &c., on aura les équations

$$mn' - m'n = h$$
$$fm + gm' + hm'' = 0$$
$$fn + gn' + hn'' = 0.$$

Mais il est inutile d'entrer dans le détail de la résolution de ces équations; car si l'on fait $my + nz = x$, $m'y + n'z = x'$, $m''y + n''z = x''$, on aura

$$\Delta = \lambda^2 x^2 + \mu^2 x'^2 + \nu^2 x''^2,$$

et les équations précédentes donneront entre $x$, $x'$, $x''$, cette relation

$$0 = fx + gx' + hx''.$$

De cette manière les coefficiens $m$, $n$, $m'$, $n'$, $m''$, $n''$, disparoissent tous du calcul, et il ne reste plus qu'à satisfaire à l'équation $fx + gx' + hx'' = 0$, au moyen de laquelle les trois indéterminées $x$, $x'$, $x''$ se réduiront à deux, et le diviseur $\Delta$, toujours de forme trinaire, se réduira anssi à la forme accoutumée $py^2 + 2qyz + rz^2$.

Pour ne laisser aucun doute sur l'exactitude du résultat précédent, il faut faire voir que les valeurs de $y$ et $z$ exprimées

au moyen de celles de $x$, $x'$, $x''$, seront toujours des entiers : or on a

$$y=\frac{n'x-nx'}{mn'-m'n}=\frac{n'x-nx'}{h}.$$

On a en même temps

$$fn+gn'+hn''=0$$
$$fx+gx'+hx''=0.$$

De ces deux dernières résulte $f(n'x-nx')+h(n'x''-n''x')=0$; il faut donc que $f(n'x-nx')$ soit divisible par $h$; mais $f$ et $h$ sont premiers entr'eux, donc $n'x-nx'$ est toujours divisible par $h$; donc $y$ est toujours un entier.

(273) De-là résulte une méthode pratique fort simple pour trouver le diviseur quadratique de la formule $t^2+cu^2$ qui répond à une valeur trinaire donnée de $c$. Soit cette valeur donnée $c=f^2\mu^2\nu^2+g^2\nu^2\lambda^2+h^2\lambda^2\mu^2$, il faudra former l'équation

$$fx+gx'+hx''=0,$$

d'après laquelle on cherchera les valeurs des trois indéterminées $x$, $x'$, $x''$, exprimées en fonctions de deux autres seulement. Ces valeurs étant trouvées, on les substituera dans la formule

$$\Delta=\lambda^2x^2+\mu^2x'^2+\nu^2x''^2,$$

qui sera le diviseur quadratique demandé.

*Exemple.* Soit la valeur donnée $c=25+81+225$, en comparant cette quantité terme à terme à la formule $f^2\mu^2\nu^2+g^2\nu^2\lambda^2+h^2\lambda^2\mu^2$, on aura $f=1$, $g=3$, $h=1$, $\nu=1$, $\mu=5$, $\lambda=3$; donc il faut faire $x+3x'+x''=0$, et le diviseur cherché sera $\Delta=9x^2+25x'^2+x''^2$. Dans ce cas on obtient immédiatement, en éliminant $x''$,

$$\Delta=9x^2+25x'^2+(x+3x')^2=10x^2+6xx'+34x'^2.$$

C'est le diviseur quadratique de la formule $t^2+cu^2$ qui répond à la valeur donnée $c=25+81+225=331$, et ce diviseur se trouve accidentellement réduit à la forme la plus simple dont il soit susceptible. Si dans le même cas on eût éliminé $x$, le diviseur $\Delta$ auroit pris la forme

$$\Delta=(9x'+3x'')^2+25x'^2+x''^2=106x'^2+54x'x''+10x''^2,$$

laquelle se simplifie par les moyens ordinaires, en mettant $y-3x'$ à la place de $x''$, et devient

$$\Delta=9y^2+25x'^2+(y-3x')^2=10y^2-6yx'+34x'^2,$$

résultat conforme au précédent.

(274) Par la forme même des équations $\Delta = \lambda^2 x^2 + \mu^2 x'^2 + \nu^2 x''^2$, $o = fx + gx' + hx''$, on voit que les lettres $f$, $g$, $h$ peuvent être échangées entr'elles, pourvu qu'on échange dans le même ordre les lettres $f$, $g$, $h$, ce qui donne toujours la même forme trinaire $c = f^2\mu^2\nu^2 + g^2\nu^2\lambda^2 + h^2\lambda^2\mu^2$. Il paroît donc que de quelque manière qu'on s'y prenne pour réduire les trois indéterminées $x$, $x'$, $x''$ à deux, on parviendra toujours à une seule et même forme pour le diviseur quadratique $\Delta$, de sorte qu'il n'y aura qu'un seul diviseur quadratique qui puisse répondre à la forme trinaire donnée. Mais cette proposition a besoin d'être mise dans un plus grand jour.

Puisque les nombres $g$ et $h$ sont premiers entr'eux, on pourra toujours en trouver deux autres $\zeta$ et $\theta$ qui satisfassent à l'équation

$$f = g\zeta + h\theta.$$

D'ailleurs puisqu'on a $o = fx + gx' + hx''$, la valeur de $f$ étant substituée dans celle-ci donnera $o = g(x' + \zeta x) + h(x'' + \theta x)$. Soit $v$ une nouvelle indéterminée, on pourra faire en général

$$x' = -\zeta x - hv$$
$$x'' = -\theta x + gv;$$

et par le moyen de ces valeurs on aura

$$\Delta = \lambda^2 x^2 + \mu^2(\zeta x + hv)^2 + \nu^2(\theta x - gv)^2;$$

de sorte que si l'on fait $\Delta = pv^2 + 2qvx + rx^2$, on aura

$$p = \mu^2 h^2 + \nu^2 g^2$$
$$q = \mu^2 \zeta h - \nu^2 \theta g$$
$$r = \lambda^2 + \mu^2\zeta^2 + \nu^2\theta^2.$$

Dans cette réduction on a conservé l'indéterminée $x$, et éliminé les deux autres $x'$, $x''$, en introduisant une nouvelle indéterminée $v$. On peut de même conserver $x'$ et éliminer $x$ et $x''$. Pour cela, soit

$$g = f\pi + h\omega,$$

et on parviendra de même au résultat

$$\Delta = \lambda^2(\pi x' + hv')^2 + \mu^2 x'^2 + \nu^2(\omega x' - fv')^2.$$

Comparant ce résultat au précédent, on fera d'abord $x' = \zeta x + hv$, $\pi x' + hv' = x$, ce qui donnera $v' = \left(\frac{1 - \pi\zeta}{h}\right)x - \pi v$. Mais des deux équations $f = g\zeta + h\theta$, $g = f\pi + h\omega$, on tire $f(1 - \pi\zeta) = h(\theta + \omega\zeta)$. Donc puisque $f$ et $h$ sont premiers entr'eux, on pourra faire $1 - \pi\zeta = h\sigma$, $\theta + \omega\zeta = f\sigma$, et on aura $v' = \sigma x - \pi v$. De-là résulte

$\omega x' - f v' = (\omega\zeta - f\sigma)x + (\omega h + f\pi)v = -\theta x + g v$. Donc le diviseur $\lambda^2(\pi x' + h v')^2 + \mu^2 x'^2 + \nu^2(\omega x' - f v')^2$ est identique avec le diviseur $\lambda^2 x^2 + \mu^2(\zeta x + h v)^2 + \nu^2(\theta x - g v)^2$. Donc il n'y a qu'un seul diviseur quadratique $py^2 + 2qyz + rz^2$ qui réponde à la forme trinaire donnée $c = f^2\mu^2\nu^2 + g^2\nu^2\lambda^2 + h^2\lambda^2\mu^2$, et on voit que ce diviseur contiendra à-la-fois les trois nombres $f^2\mu^2 + g^2\lambda^2$, $f^2\nu^2 + h^2\lambda^2$, $g^2\nu^2 + h^2\mu^2$.

(275) Il reste à examiner quels sont les cas où le diviseur quadratique $\Delta$ pourra se décomposer de plusieurs manières en trois quarrés, sans cesser de correspondre à la valeur trinaire donnée de $c$. Et d'abord on s'assurera par plusieurs exemples que la chose est possible ; car en faisant $c = 16 + 4 + 1$, le diviseur correspondant de la formule $t^2 + 21u^2$ est $5y^2 + 6yz + 6z^2$, lequel se décompose en trois quarrés de ces deux manières :

$$(2y+z)^2 + (y+z)^2 + 4z^2$$
$$(y-z)^2 + z^2 + (2y+2z)^2 ;$$

et de chacune de ces décompositions on déduira, d'après la formule du n°. 268, la même valeur trinaire $c = 16 + 4 + 1$. Il s'agit donc de déterminer quels sont les cas qui donnent lieu à cette multiplicité de formes trinaires d'un même diviseur quadratique.

Soit $py^2 + 2qyz + rz^2$ l'expression la plus simple du diviseur quadratique $\Delta$, et soit conformément à la forme générale (n°. 271) $\Delta = \lambda^2(my + nz)^2 + \mu^2(m'y + n'z)^2 + \nu^2(m''y + n''z)^2$, on aura

$$p = \lambda^2 m^2 + \mu^2 m'^2 + \nu^2 m''^2$$
$$q = \lambda^2 m n + \mu^2 m' n' + \nu^2 m'' n''$$
$$r = \lambda^2 n^2 + \mu^2 n'^2 + \nu^2 n''^2.$$

Et pour que la forme trinaire supposée corresponde à la valeur donnée de $c$, il faut de plus satisfaire aux équations

$$m n' - m' n = h$$
$$f m + g m' + h m'' = 0$$
$$f n + g n' + h n'' = 0.$$

Soit comme ci-dessus $f = g\zeta + h\theta$, les deux dernières équations donneront, en prenant deux nouvelles indéterminées $M$, $N$ :

$$m' = -\zeta m + h M \qquad n' = -\zeta n + h N$$
$$m'' = -\theta m - g M \qquad n'' = -\theta n - g N.$$

Ces valeurs étant substituées dans la première $mn'-m'n=h$, il ne restera plus qu'à satisfaire à la condition

$$mN-nM=1;$$

et tont ce qui concerne les coefficiens $m, n, m', n', m'', n''$ sera censé déterminé. Maintenant si l'on substitue les valeurs de ces coefficiens dans celles de $p, q, r$, et qu'on fasse pour abréger

$$\begin{aligned} A &= \lambda^2+\mu^2\zeta^2+\nu^2\theta^2 \\ B &= \mu^2\zeta h-\nu^2\theta g \\ C &= \mu^2h^2+\nu^2g^2, \end{aligned}$$

on aura

$$\begin{aligned} p &= Am^2-2BmM+CM^2 \\ q &= Amn-B(mN+nM)+CMN \\ r &= An^2-2BnN+CN^2. \end{aligned}$$

Mais comme on a déjà exprimé la condition $pr-q^2=c$, on peut faire abstraction de la seconde équation, et ne considérer que les deux autres :

$$\begin{aligned} p &= Am^2-2BmM+CM^2 \\ r &= An^2-2BnN+CN^2. \end{aligned}$$

Il faudra donc qu'on puisse satisfaire de plusieurs manières à celles-ci, s'il y a plusieurs formes trinaires du diviseur $\Delta$ qui répondent à la valeur trinaire donnée de $c$.

(276) J'observe que la formule indéterminée $Ay^2-2Byz+Cz^2$ satisfait à la condition $AC-B^2=c$; elle représente donc un diviseur quadratique de la formule $t^2+cu^2$. De plus, cette formule, ainsi qu'on le voit par les valeurs de ses coefficiens (conformes à celles de $p, q, r$ dans le n°. 274), est le diviseur qui répond à la forme trinaire donnée de $c$; elle doit donc avoir pour expression la plus simple $py^2-2qyz+rz^2$.

Mais un même nombre ne peut être représenté de deux manières par la formule $Ay^2-2Byz+Cz^2$, sans l'être aussi de deux manières par la formule équivalente $py'^2-2qy'z'+rz'^2$. Car de la première on passe à la seconde, en faisant $y=\alpha y'+\alpha^\circ z'$, $z=\beta y'+\beta^\circ z'$, et supposant $\alpha\beta^\circ-\alpha^\circ\beta=1$. Donc s'il n'y avoit qu'une manière de satisfaire à l'équation $K=py'^2-2qy'z'+rz'^2$, il n'y auroit non plus qu'une solution de l'équation $K=Ay^2-2Byz+Cz^2$. Donc

Donc si le diviseur quadratique $py^2+2qyz+rz^2$ se décompose de plusieurs manières en trois quarrés, et qu'en même temps ces diverses formes trinaires répondent à une même forme donnée du nombre $c$, il faudra que l'une au moins des deux équations $p=py^2-2qyz+rz^2$, $r=py^2-2qyz+rz^2$ admette un pareil nombre de solutions. Et il faut remarquer que comme on peut changer à-la-fois les signes de $y$ et de $z$, on ne doit regarder comme solutions différentes que celles qui donneroient pour $\frac{y}{z}$ des valeurs différentes.

Mais puisque le second membre est réduit à l'expression la plus simple, il n'y aura qu'un nombre de cas très-limité où l'on pourra avoir deux solutions et jamais plus. Ce sont 1°. le cas de $p=r$ où l'on peut faire $y=0$, $z=1$, ou $y=1$, $z=0$; 2°. le cas de $r=2q$ où l'on peut avoir de deux manières $p=py^2-2qyz+2qz^2$, l'une en faisant $y=1$, $z=0$, l'autre en faisant $y=1$, $z=1$; 3°. le cas de $p=2q$ qui est semblable au précédent.

Au reste, on peut voir immédiatement, dans ces différens cas, qu'il y a, ou qu'il peut y avoir deux formes trinaires du diviseur quadratique, lesquelles correspondent à une même valeur de $c$.

En effet, 1°. si l'on a $p=r$, les indéterminées $y$ et $z$ pourront être échangées entr'elles, et le diviseur $py^2+2qyz+pz^2$ qui se décompose en ces trois quarrés $\lambda^2(my+nz)^2+\mu^2(m'y+n'z)^2+\nu^2(m''y+n''z)^2$, se décomposera également en ces trois autres, $\lambda^2(mz+ny)^2+\mu^2(m'z+n'y)^2+\nu^2(m''z+n''y)^2$, seconde forme qui pourra être différente de la première, et qui cependant répondra à la même valeur trinaire de $c$. C'est ainsi que le diviseur $10y^2+6yz+10z^2$ qui appartient à la formule $t^2+91u^2$, se décompose en trois quarrés de ces deux manières :

$$y^2+9z^2+(3y+z)^2$$
$$z^2+9y^2+(3z+y)^2,$$

lesquelles répondent à la même forme trinaire $c=81+9+1$.

2°. Si l'on a $r=2q$, on pourra dans le diviseur quadratique $py^2+2qyz+2qz^2$ changer $z$ en $-z-y$; donc si ce diviseur est de la forme $\lambda^2(my+nz)^2+\mu^2(m'y+n'z)^2+\nu^2(m''y+n''z)^2$, il sera en

même temps de la forme $\lambda^2(my-ny-nz)^2+\mu^2(m'y-n'y-n'z)^2+\nu^2(m''y-n''y-n''z)^2$.

3°. Le cas de $p=2q$ est semblable au précédent, et on pourroit y ramener aussi le cas de $p=r$, car en substituant $y-z$ à $y$, la formule $py^2+2qyz+pz^2$ devient $py^2+(2q-2p)yz+(2p-2q)z^2$.

Enfin à ces différens cas, il faut joindre celui où le diviseur quadratique $\Delta$ seroit de la forme $py^2+2pyz+rz^2$, ou simplement $py^2+rz^2$, c'est-à-dire le cas de $q=p$ ou $q=0$. Car lorsque $q=0$, il est clair qu'on peut changer le signe de $z$; donc le diviseur $py^2+rz^2$ qui est de la forme $\lambda^2(my+nz)^2+\mu^2(m'y+n'z)^2+\nu^2(m''y+n''z)^2$, sera en même temps de la forme $\lambda^2(my-nz)^2+\mu^2(m'y-n'z)^2+\nu^2(m''y-n''z)^2$, et ces deux formes trinaires répondront toujours à la même valeur trinaire de $c$.

(277) Il résulte de tout ce qu'on vient de démontrer, qu'étant donnée la forme trinaire $c=f^2\mu^2\nu^2+g^2\nu^2\lambda^2+h^2\lambda^2\mu^2$, dont les trois termes ne sont pas divisibles par un même quarré, si l'on veut trouver le diviseur trinaire correspondant de la formule $t^2+cu^2$;

1°. Ce diviseur sera donné par la formule $\lambda^2x^2+\mu^2x'^2+\nu^2x''^2$, où les indéterminées $x$, $x'$, $x''$ doivent être réduites à deux d'après l'équation $fx+gx'+hx''=0$.

2°. De quelque manière qu'on fasse cette réduction, le résultat, ramené à l'expression la plus simple, sera toujours le même, il ne pourra donc y avoir qu'un seul diviseur quadratique $py^2+2qyz+rz^2$, qui satisfasse à la question.

3°. Ce diviseur ne pourra se décomposer en trois quarrés correspondans à la forme trinaire donnée de $c$, que d'une seule manière, excepté dans les cas ci-après désignés où il pourra y avoir deux décompositions.

Lorsque $q=0$, on pourra, dans la forme trinaire du diviseur, changer le signe de $z$.

Le cas de $q=p$ revient au précédent, parce que la formule $py^2+2pyz+rz^2$ se réduit à $py'^2+(r-p)z^2$; il est donc aussi susceptible d'une seconde solution, laquelle se trouve directement, en mettant $-y-2z$ à la place de $y$ dans la valeur de $py^2+2pyz+rz^2$.

Lorsque $p=r$, les quantités $y$ et $z$ pourront être échangées l'une dans l'autre.

Lorsque $2q=r$, on pourra mettre $-y-z$ à la place de $z$, et lorsque $2q=p$, on mettra $-y-z$ à la place de $y$.

Dans ces cas, par conséquent, il pourra y avoir deux formes trinaires du diviseur cherché, lesquelles répondront à la valeur donnée de $c$. Mais comme on a supposé que les trois termes composant la valeur de $c$ ne sont pas divisibles par un même nombre, on peut, en ayant égard à cette condition, déterminer d'une manière précise les cas où le diviseur cherché aura nécessairement deux formes trinaires, et ceux où il n'en aura qu'une.

(278) Soit d'abord le diviseur trinaire dont il s'agit : $\Delta=py^2+2qyz+pz^2=(My+Nz)^2+(M'y+N'z)^2+(M''y+N''z)^2$, je dis qu'en changeant $y$ et $z$ l'un dans l'autre, on aura toujours une nouvelle forme trinaire de $\Delta$ correspondante à la même valeur trinaire de $c$.

Car si la forme trinaire du diviseur $\Delta$ restoit la même, malgré le changement des indéterminées, il faudroit que les trois quarrés $(My+Nz)^2+(M'y+N'z)^2+(M''y+N''z)^2$ fussent identiques avec les trois $(Mz+Ny)^2+(M'z+N'y)^2+(M''z+N''y)^2$. Or la seule combinaison dans laquelle cette identité seroit possible, donne

$$\Delta=(My+Nz)^2+(Mz+Ny)^2+(M'y\pm M'z)^2;$$

et il en résulte pour valeur correspondante de $c$ :

$$c=(MM-NN)^2+(MM'\mp NM')^2+(MM'\mp NM')^2.$$

Mais comme les trois termes de cette expression sont divisibles par $(M\mp N)^2$, il faut, pour ne pas sortir de notre hypothèse, faire $M\mp N=1$, et alors on aura

$$c=(M\pm N)^2+M'^2+M'^2.$$

Si l'on fait en même temps $z=z'\mp y$, on aura

$$\Delta=(y\mp Mz')^2+(y+Nz)^2+M'^2z'^2=2y^2\mp 2yz'+\frac{c+1}{2}z'^2.$$

Or cette forme ne peut s'accorder avec la forme primitivement supposée $py^2+2qyz+pz^2$, à moins de faire $c=3$, cas dont on peut faire abstraction. Donc toutes les fois que le diviseur qua-

dratique $\Delta$ sera de la forme $py^2+2qyz+pz^2$, il y aura toujours deux formes trinaires du diviseur $\Delta$, lesquelles répondront à la même valeur trinaire de $c$.

Le cas où le diviseur quadratique seroit $py^2+2qyz+2qz^2$, mène à une semblable conclusion, parce qu'en mettant $y-z$ à la place de $y$, il prend la forme $py^2+(2p-2q)yz+pz^2$ semblable à celle qu'on vient d'examiner. Il y aura donc alors deux formes trinaires du même diviseur correspondantes à une même valeur trinaire de $c$; il faut excepter seulement le cas où $q=1$; car le diviseur $py^2+2yz+2z^2$ décomposé en trois quarrés, ne peut être que de la forme

$$(z+(a+1)y)^2+(z-ay)^2+b^2y^2,$$

laquelle ne change pas en mettant $-z-y$ à la place de $z$.

Il ne reste plus qu'à examiner le cas de $q=0$, auquel se ramèneroit le cas de $q=p$; alors le diviseur $py^2+rz^2$ sera à-la-fois des deux formes $(My+Nz)^2+(M'y+N'z)^2+(M''y+N''z)^2$ et $(My-Nz)^2+(M'y-N'z)^2+(M''y-N''z)^2$, lesquelles répondront à une même valeur trinaire de $c$; et ces deux formes seront toujours différentes l'une de l'autre, à moins que le diviseur dont il s'agit ne soit $(My+Nz)^2+(My-Nz)^2+(M'y)^2$. Dans ce cas particulier, on aura $c=(2MN)^2+(M'N)^2+(M'N)^2$, et pour éviter le facteur commun il faudra faire $N=1$, ce qui donnera $c=4M^2+2M'^2$, et $py^2+rz^2=2z^2+\frac{c}{2}y^2$; de sorte qu'il y a exception seulement lorsque $p=2$.

(279) On peut donc établir, pour conclusion générale, que la forme trinaire donnée du nombre $c$ ne répondra qu'à une seule forme trinaire du diviseur quadratique qui en est déduit, tant qu'on n'aura pas une des égalités $q=0$ ou $p$, $p=r$, $2q=p$ ou $r$. Mais si l'une de ces égalités a lieu, et qu'en même temps le moindre des deux nombres $p$ et $r$ ne soit ni 1 ni 2, il y aura deux formes trinaires du même diviseur $py^2+2qyz+rz^2$, lesquelles répondront à la valeur donnée de $c$.

*Remarque*. Il est bon d'observer que le même diviseur quadratique peut avoir diverses formes trinaires correspondantes à diverses

formes trinaires du nombre $c$ : mais la même forme trinaire de $c$ ne répondra jamais à plus de deux formes trinaires du même diviseur quadratique, et cela n'aura lieu que dans les cas précités.

Par exemple, la formule $t^2+77u^2$ a pour l'un de ses diviseurs quadratiques $13y^2+2yz+6z^2$, lequel se décompose en trois quarrés de ces deux manières :

$$(3y+z)^2+(2y-z)^2+4z^2$$
$$(3y-z)^2+(2y+2z)^2+z^2;$$

or la première forme répond à la forme trinaire $77=5^2+6^2+4^2$, et la seconde à la forme trinaire $77=8^2+3^2+2^2$.

De même le diviseur $5y^2+21z^2$, l'un de ceux de la formule $t^2+105u^2$, se décompose en trois quarrés de quatre manières, dont deux répondent à la forme trinaire $105=10^2+2^2+1^2$, et les deux autres à la forme trinaire $105=8^2+5^2+4^2$. Voici cette correspondance :

$$c=10^2+2^2+1^2 \qquad \Delta=(2y+2z)^2+(y-4z)^2+z^2$$
$$c=10^2+2^2+1^2 \qquad \Delta=(2y-2z)^2+(y+4z)^2+z^2$$

$$c=\ 8^2+5^2+4^2 \qquad \Delta=(2y+z)^2+(y-2z)^2+16z^2$$
$$c=\ 8^2+5^2+4^2 \qquad \Delta=(2y-z)^2+(y+2z)^2+16z^2.$$

(280) Tout ce qui précède suppose que les trois quarrés composant la valeur donnée de $c$ n'ont point de facteur commun ; nous examinerons aussi succinctement le cas où ces trois quarrés auroient un facteur commun $\psi^2$; alors toutes choses restant les mêmes, on pourra représenter la valeur donnée de $c$ par la formule

$$c=(f^2\mu^2\nu^2+g^2\nu^2\lambda^2+h^2\lambda^2\mu^2)\psi^2.$$

Soit toujours le diviseur quadratique correspondant

$$\Delta=\lambda^2(my+nz)^2+\mu^2(m'y+n'z)^2+\nu^2(m''y+n''z)^2,$$

et il ne s'agira plus que de satisfaire aux trois équations

$$mn'-m'n=h\psi$$
$$fm+gm'+hm''=0$$
$$fn+gn'+hn''=0.$$

On pourroit, comme dans le cas précédent, réduire la valeur de $\Delta$ à la forme

$$\Delta=\lambda^2x^2+\mu^2x'^2+\nu^2x''^2,$$

et déterminer l'une des quantités $x$, $x'$, $x''$ par l'équation
$$0 = fx + gx' + hx''.$$
Mais cette condition ne seroit pas suffisante, car il faut que les valeurs de $y$ et $z$ tirées des équations $my + nz = x$, $m'y + n'z = x'$, soient des entiers ; ces valeurs sont :
$$y = \frac{n'x - nx'}{mn' - m'n}, \quad z = \frac{mx' - m'x}{mn' - m'n}.$$
Or on prouvera comme ci-dessus que les quantités $n'x - nx'$ et $mx' - m'x$ sont divisibles par $h$; mais il faut encore qu'elles le soient par $\psi$, puisque $mn' - m'n = h\psi$; nouvelle condition qui exige qu'on poursuive la résolution des équations en $m$, $n$, $m'$, &c.

Soit comme ci-dessus $f = g\zeta + h\theta$, on pourra faire de même (n°. 275)
$$m' = -\zeta m + hM \qquad n' = -\zeta n + hN$$
$$m'' = -\theta m - gM \qquad n'' = -\theta n - gN,$$
et on aura l'équation de condition $mN - nM = \psi$, de laquelle seule dépendent les indéterminées restantes $m$, $n$, $M$, $N$. Soit $\psi = \alpha\mathcal{C}$, si l'on fait $m = \alpha M'$, $n = \alpha N'$, l'équation de condition sera $M'N - N'M = \mathcal{C}$, et comme $M'$ et $N'$ peuvent maintenant être considérés comme premiers entr'eux, on pourra faire
$$M'A - N'B = 1,$$
ce qui donnera $M = B\mathcal{C} + M'\sigma$, $N = A\mathcal{C} + N'\sigma$, $\sigma$ étant une nouvelle indéterminée. Au moyen de ces valeurs on aura
$$my + nz = \alpha(M'y + N'z)$$
$$m'y + n'z = (h\sigma - \zeta\alpha)(M'y + N'z) + h\mathcal{C}(By + Az)$$
$$m''y + n''z = -(g\sigma + \theta\alpha)(M'y + N'z) - g\mathcal{C}(By + Az).$$
Mais on peut faire $M'y + N'z = z'$ et $By + Az = y'$, parce qu'ayant $M'A - N'B = 1$, les valeurs de $y$ et $z$ exprimées en $y'$ et $z'$ seront des nombres entiers; donc enfin le diviseur cherché sera (après avoir effacé les accens)
$$\Delta = \lambda^2\alpha^2z^2 + \mu^2((h\sigma - \zeta\alpha)z + h\mathcal{C}y)^2 + \nu^2((g\sigma + \theta\alpha)z + g\mathcal{C}y)^2.$$
Cette forme générale contient autant de formes particulières qu'il y a de manières de partager $\psi$ en deux facteurs $\alpha$ et $\mathcal{C}$; de plus, chaque forme particulière pourra se subdiviser en plusieurs autres, à cause de l'indéterminée $\sigma$ qui y est contenue.

On prouvera aisément par la formule du n°. 268 qu'en effet

l'expression générale du diviseur quadratique qu'on vient de trouver reproduit la forme donnée $c=(f^2\mu^2\nu^2+g^2\nu^2\lambda^2+h^2\lambda^2\mu^2)\psi^2$, ainsi il ne peut y avoir de doute sur la solution précédente, et on en conclura qu'il existe toujours plusieurs diviseurs quadratiques trinaires qui répondent à une forme trinaire donnée du nombre $c$, lorsque les trois quarrés qui composent cette forme ont un diviseur commun $\psi^2$. Résultat qui établit une différence essentielle entre le cas où les trois quarrés donnés ont un commun facteur, et celui où ils n'en ont pas.

(281) Soit par exemple la forme donnée $81+36+36=153=c$, on aura $\psi=3$, $f=3$, $gh\mu\nu=1$, $\lambda=2$, et l'équation pour déterminer $\zeta$ et $\theta$ sera $3=\zeta+\theta$, laquelle donne $\theta=3$, $\zeta=0$. Ensuite, comme on a $3=\alpha\mathcal{C}$, il n'y a que deux suppositions à faire, l'une $\alpha=1$, $\mathcal{C}=3$, l'autre $\alpha=3$, $\mathcal{C}=1$; de-là on tire les deux formes suivantes du diviseur quadratique cherché :

$$\Delta=36z^2+(\sigma z+y)^2+((\sigma+9)z+y)^2$$
$$\Delta=\ 4z^2+(\sigma z+3y)^2+((\sigma+3)z+3y)^2.$$

La première se réduit toujours, quel que soit $\sigma$, à la seule forme

$$\Delta=(y+5z)^2+(y-4z)^2+36z^2=2y^2+2yz+77z^2.$$

La seconde fournit les deux formes

$$\Delta=4z^2+(3z+3y)^2+(3y)^2=13z^2+18yz+18y^2$$
$$\Delta=4z^2+(2z+3y)^2+(z-3y)^2=9z^2+6yz+18y^2.$$

Il y a donc en tout trois diviseurs quadratiques différens qui répondent à la forme trinaire donnée $81+36+36$.

## §. IV. *Suite des Théorêmes relatifs aux diviseurs trinaires.*

(282) Théorème V. *Si le diviseur quadratique* $py^2+2qyz+2\pi z^2$ *est trinaire ou décomposable en trois quarrés, le double de son conjugué sera également décomposable en trois quarrés.*

Car soieut $\Delta$ le premier diviseur et $\Gamma$ son conjugué $2py^2+2qyz+\pi z^2$, on aura $2\Gamma=4py^2+4qyz+2\pi z^2$, quantité qui n'est autre chose que la fonction $\Delta=py^2+2qyz+2\pi z^2$ dans laquelle au lieu de $y$ on mettroit $2y$. Donc si l'on a

$$\Delta=(my+nz)^2+(m'y+n'z)^2+(m''y+n''z)^2,$$

il s'ensuivra

$$2\Gamma=(2my+nz)^2+(2m'y+n'z)^2+(2m''y+n''z)^2,$$

et ainsi $2\Gamma$ est décomposable en trois quarrés.

Il résulte de-là différentes conséquences. 1°. Si le nombre $c$ est de forme $8k+5$, on a déjà vu (n°. 215) que le diviseur $\Delta$ doit être compris parmi les diviseurs $4x+1$, et son conjugué $\Gamma$ parmi les diviseurs $4x-1$. Donc autant il y aura de diviseurs quadratiques $4x+1$ décomposables en trois quarrés, autant il y aura de diviseurs quadratiques $4x-1$, dont le double est décomposable aussi en trois quarrés.

2°. Si le nombre $c$ est de forme $8k+1$, les deux diviseurs conjugués $\Delta$ et $\Gamma$ se trouveront à-la-fois parmi les diviseurs $4x+1$. Donc si un diviseur quadratique $4x+1$ est de forme trinaire, il y aura toujours un autre diviseur quadratique $4x+1$ dont le double sera d'une semblable forme.

(283) Théorème VI. *Si* c *est un nombre premier, ou le double d'un tel nombre, la formule* $t^2+cu^2$ *aura autant de diviseurs trinaires qu'il y a de formes trinaires du nombre* c.

Car chaque forme trinaire du nombre $c$ fournit un diviseur trinaire de la formule $t^2+cu^2$, et n'en fournit qu'un (n°. 277), puisque $c$ n'est divisible par aucun quarré. D'un autre côté, deux formes trinaires

trinaires différentes du nombre $c$ ne peuvent conduire à une même forme de diviseur trinaire, tant que $c$ ou $\frac{1}{2}c$ est un nombre premier. Car soient deux formes trinaires différentes

$$c = f^2 + (\mu^2 + \nu^2) g^2$$
$$c = f'^2 + (\mu'^2 + \nu'^2) g'^2,$$

dans lesquelles $\mu$ et $\nu$ sont premiers entr'eux, ainsi que $\mu'$ et $\nu'$; si ces deux formes conduisoient à un même diviseur quadratique, ce diviseur (n°. 274) contiendroit à-la-fois les deux nombres $\mu^2 + \nu^2$, $\mu'^2 + \nu'^2$. Or d'après le théorême II cela ne peut avoir lieu, à moins que les trois quarrés $f^2 + g^2\mu^2 + g^2\nu^2$ ne soient les mêmes, à l'ordre près, que les trois quarrés $f'^2 + g'^2\mu'^2 + g'^2\nu'^2$, et alors ces deux formes coincideroient en une seule, contre la supposition. Donc les diverses formes trinaires dont $c$ est susceptible donneront un pareil nombre de diviseurs trinaires de la formule $t^2 + cu^2$, tous différens les uns des autres. D'ailleurs il ne peut y avoir (n°. 268) aucun diviseur trinaire qui ne réponde à une valeur trinaire de $c$. Donc *si* c *est premier*, &c.

(284) Théorême VII. *Si le nombre* c *est premier ou double d'un premier, tout diviseur trinaire de la formule* $t^2 + cu^2$, *ne pourra se décomposer en trois quarrés que d'une seule manière.*

Car si un diviseur quadratique étoit décomposable de plusieurs manières en trois quarrés, il faudroit, d'après la démonstration précédente, que ces diverses décompositions répondissent à une même valeur trinaire de $c$. Mais on a prouvé (n°. 279) que deux valeurs trinaires de $c$ ne peuvent répondre à une même forme trinaire d'un diviseur quadratique, à moins que celui-ci ne soit de l'une des formes $py^2 + rz^2$, $py^2 + 2qyz + pz^2$, $py^2 + 2qyz + 2qz^2$, et qu'en outre les coefficiens extrêmes soient l'un et l'autre plus grands que 2. Or, dans ces différens cas, il est facile de voir que le nombre $c$, représenté successivement par $pr$, $p^2 - q^2$, $2pq - q^2$, ne peut être ni premier, ni double de premier. Donc si $c$ est premier ou double d'un premier, il n'y aura jamais qu'une manière de décomposer en trois quarrés tout diviseur trinaire de la formule $t^2 + cu^2$.

*Remarque.* Cette proposition présente une propriété qui convient exclusivement aux nombres premiers ou doubles de premiers, et qui peut servir à distinguer ces nombres de tous les autres. En effet, dans tous les cas où $c$ sera un nombre composé, autre que le double d'un nombre premier, on trouvera que le diviseur $py^2+2qyz+rz^2$, s'il est trinaire ou décomposable en trois quarrés, le sera toujours de plusieurs manières. Par exemple, la formule $t^2+321u^2$ a pour diviseur trinaire $17y^2+22yz+26z^2$, et ce diviseur, parce que 321 est le produit de deux nombres premiers 3,107, se décompose en trois quarrés de ces deux manières :

$$17y^2+22yz+26z^2=\begin{cases}(4y+3z)^2+(y-z)^2+4z^2\\(2y+3z)^2+(3y-z)^2+(2y+4z)^2\end{cases}$$

où l'on observera que la première forme trinaire $(4y+3z)^2+(y-z)^2+4z^2$ du diviseur répond (n°. 268) à la valeur trinaire $321=7^2+16^2+4^2$, et la seconde forme trinaire du diviseur à une seconde valeur trinaire de 321, savoir, $321=11^2+2^2+14^2$.

(285) THÉORÈME VIII. *Si le nombre* N *est compris dans un diviseur trinaire de la formule* $t^2+cu^2$, *réciproquement le nombre* c *sera compris dans un diviseur trinaire de la formule* $t^2+Nu^2$. *De plus, les valeurs trinaires de* N *et de* c, *déduites de l'un ou de l'autre diviseur, seront identiques.*

Pour bien faire saisir le sens de la seconde partie, considérons la formule $t^2+65u^2$ et son diviseur quadratique $9y^2+10yz+10z^2$, dont une forme trinaire est $(2y+3z)^2+(2y)^2+(y-z)^2$. Si dans ce diviseur on fait $y=3$, $z=2$, on aura le nombre compris $181=12^2+6^2+1^2$; cette même forme trinaire $(2y+3z)^2+(2y)^2+(y-z)^2$ donne pour la valeur correspondante de $c$ (n°. 268), $65=6^2+2^2+5^2$. Réciproquement parmi les diviseurs quadratiques de la formule $t^2+181u^2$, on en trouve un $5y^2+4yz+37z^2$ qui contient le nombre 65, et duquel 65 résulte en faisant $y=2$, $z=1$. Or ce diviseur peut se mettre sous la forme $y^2+(6z)^2+(2y+z)^2$, de laquelle on déduit, tant pour 181 que pour 65, les valeurs trinaires $65=2^2+6^2+5^2$, $181=12^2+6^2+1^2$, entièrement semblables à celles qui ont été tirées du premier diviseur.

Cela posé, soit en général $\Delta$ un diviseur quadratique de la formule $t^2+cu^2$, lequel se décompose en trois quarrés de cette manière :

$$\Delta=(my+nz)^2+(m'y+n'z)^2+(m''y+n''z)^2,$$

la valeur trinaire de $c$ correspondante à cette forme sera

$$c=(mn'-m'n)^2+(m'n''-m''n')^2+(m''n-mn'')^2.$$

Soit $N$ un nombre quelconque compris dans le diviseur $\Delta$, on pourra supposer

$$N=(m\alpha+n\beta)^2+(m'\alpha+n'\beta)^2+(m''\alpha+n''\beta)^2;$$

et telles sont, dans le sens du théorême, les valeurs trinaires de $N$ et de $c$ déduites du diviseur $\Delta$.

Cherchons maintenant, d'après cette valeur de $N$, le diviseur correspondant de la formule $t^2+Nu^2$, et pour cela nous supposerons d'abord que les trois termes composant la valeur de $N$ ne sont pas divisibles par un même nombre. Nous ferons donc, suivant la méthode développée dans le §. précédent,

$$m\alpha+n\beta=f\mu\nu$$
$$m'\alpha+n'\beta=g\nu\lambda$$
$$m''\alpha+n''\beta=h\lambda\mu,$$

ce qui donnera $N=f^2\mu^2\nu^2+g^2\nu^2\lambda^2+h^2\lambda^2\mu^2$, et le diviseur trinaire de la formule $t^2+Nu^2$ correspondant à cette valeur, sera $\Gamma=\lambda^2x^2+\mu^2x'^2+\nu^2x''^2$ : formule où les indéterminées $x$, $x'$, $x''$, doivent satisfaire à la condition $fx+gx'+hx''=0$. Il reste donc à prouver que le nombre $c$ est compris dans le diviseur $\Gamma$, et qu'il y est compris sous la forme trinaire déjà trouvée. Or les équations ci-dessus donnent :

$$(mn'-m'n)\alpha=\nu(f\mu n'-g\lambda n),\quad (mn'-m'n)\beta=\nu(g\lambda m-f\mu m')$$
$$(m'n''-m''n')\alpha=\lambda(g\nu n''-h\mu n'),\quad (m'n''-m''n')\beta=\lambda(h\mu m'-g\nu m'')$$
$$(m''n-mn'')\alpha=\mu(h\lambda n-f\nu n''),\quad (m''n-mn'')\beta=\mu(f\nu m''-h\lambda m),$$

et comme on suppose toujours $\alpha$ et $\beta$ premiers entr'eux, on pourra déterminer $A$ et $B$ d'après l'équation $\alpha A-\beta B=1$ ; puis faisant pour abréger,

$$k=A(g\nu n''-h\mu n')-B(h\mu m'-g\nu m'')$$
$$k'=A(h\lambda n-f\nu n'')-B(f\nu m''-h\lambda m)$$
$$k''=A(f\mu n'-g\lambda n)-B(g\lambda m-f\mu m'),$$

on aura

$$m n' - m'n = \nu k''$$
$$m'n'' - m''n' = \lambda k$$
$$m''n - m n'' = \mu k' ;$$

de sorte que la valeur trinaire de $c$ deviendra $c = \lambda^2 k^2 + \mu^2 k'^2 + \nu^2 k''^2$. Enfin il est aisé de voir que les valeurs de $k$, $k'$, $k''$, substituées dans l'équation $fk + gk' + hk'' = 0$, la rendent identique ; de plus, les trois nombres $k$, $k'$, $k''$ ne sont pas divisibles par un même facteur $\psi$ ; car si cela étoit, les trois quarrés qui composent la valeur de $c$ seroient divisibles par $\psi^2$, contre la supposition. Donc le nombre $c$ est compris dans le diviseur $\lambda^2 x^2 + \mu^2 x'^2 + \nu^2 x''^2$ qui appartient à la formule $t^2 + Nu^2$, et il y est compris sous la même forme trinaire qu'avoit déjà donnée le diviseur $\Delta$ de la formule $t^2 + cu^2$.

(286) Nous avons supposé dans la démonstration précédente, que les trois quarrés qui composent le nombre $N$ n'ont pas de commun diviseur ; s'ils en avoient un, on feroit

$$m\alpha + n\beta = f\mu\nu\psi$$
$$m'\alpha + n'\beta = g\nu\lambda\psi$$
$$m''\alpha + n''\beta = h\lambda\mu\psi ;$$

et toutes choses restant d'ailleurs les mêmes, on auroit

$$m n' - m'n = \nu\psi k''$$
$$m'n'' - m''n' = \lambda\psi k$$
$$m''n - m n'' = \mu\psi k',$$

les quantités $k, k', k''$ ayant toujours les mêmes valeurs que ci-dessus ; d'où l'on voit qu'alors la valeur de $c$ seroit

$$c = \psi^2 (\lambda^2 k^2 + \mu^2 k'^2 + \nu^2 k''^2),$$

et qu'ainsi les trois quarrés qui composent $c$ auroient le même diviseur commun $\psi^2$ que les trois quarrés qui composent $N$. Donc lorsque les trois quarrés qui composent $c$, et d'après lesquels le diviseur quadratique de $t^2 + cu^2$ est déterminé, n'auront pas de diviseur commun, il arrivera toujours que les trois quarrés qui composent $N$ n'auront pas non plus de diviseur commun. Car si ceux-ci en avoient un, on voit que le même commun diviseur se retrouveroit daus la valeur de $c$.

Au reste, dans le cas même où les quarrés qui composent $N$ ont un diviseur commun $\psi^2$ qui divise en même temps les trois quarrés

composant $c$, il sera toujours vrai de dire que si $N$ est compris dans un diviseur trinaire de $t^2+cu^2$, réciproquement $c$ sera compris dans un diviseur trinaire de $t^2+Nu^2$. Car alors faisant $N=\psi^2N'$ et $c=\psi^2c'$, il est clair que si $N'$ est diviseur de $t^2+c'u^2$, il s'ensuit que $N$ est diviseur de $t^2+cu^2$; et si en même temps $c'$ est diviseur de $t^2+N'u^2$, il s'ensuivra également que $c$ est diviseur de $t^2+Nu^2$.

Toujours est-il nécessaire, si les trois quarrés qui composent $c$ ont un facteur commun $\psi^2$, que les trois quarrés qui composent $N$ aient le même commun diviseur, sans quoi il ne pourra se faire que $c$ divise $t^2+Nu^2$. Mais on voit en même temps que les facteurs communs, lorsqu'il y en a, sont en quelque sorte étrangers à la propriété dont il s'agit, et qu'ils n'apportent aucun changement à la proposition principale, dans laquelle on peut supposer constamment que les trois quarrés composant $c$ n'ont point de facteur commun. Et de cette supposition il s'ensuivra nécessairement que les trois quarrés composant $N$ n'auront pas non plus de facteur commun.

Il est à remarquer, au reste, que cette supposition n'exclut pas le cas où le nombre $c$ seroit quarré ou divisible par un quarré. Car rien n'empêche qu'un nombre qui est quarré ou divisible par un quarré, ne soit composé de trois quarrés qui n'ont pas de commun diviseur; tels sont $9=4+4+1$, $45=25+16+4$, et ainsi des autres. D'où il suit qu'il n'y a non plus aucune valeur de $N$ exclue. Voici des exemples qui ne laisseront là-dessus aucun doute.

(287) Le nombre 117 étant mis sous la forme trinaire $100+16+1$, le diviseur de $t^2+117u^2$ correspondant à cette forme est

$$9y^2+6yz+14z^2=(2y+3z)^2+(2y-2z)^2+(y+z)^2.$$

Je prends à dessein le nombre 9 compris dans ce diviseur, et comme 9 se trouve en faisant $y=1$, $z=0$, je substitue ces valeurs dans la forme trinaire du diviseur indéterminé, et j'ai la forme trinaire $4+4+1$ pour le diviseur déterminé 9. Je cherche ensuite, par les méthodes précédentes, le diviseur de $t^2+9u^2$ qui répond à cette forme, je trouve

$$2y^2+2yz+5z^2=y^2+(y+z)^2+4z^2.$$

Il faut donc réciproquement que le nombre 117 se trouve compris dans

ce diviseur. En effet, si l'on forme l'équation $117=2y^2+2yz+5z^2$, et qu'ensuite on la multiplie par 2, on aura $234=(2y+z)^2+9z^2$, ou $26=\left(\frac{2y+z}{3}\right)^2+z^2$. Soit donc $z=1$, on aura $\frac{2y+z}{3}=\pm 5$, ce qui donnera $y=7$ ou $-8$, valeurs d'où résulte également $2y^2+2yz+5z^2=117=8^2+7^2+2^2$. Cette valeur n'est pas la forme trinaire donnée ; mais on peut obtenir une autre solution en faisant $z=5$, $\frac{2y+z}{3}=\pm 1$, ce qui donnera $y=-1$ ou $-4$, et alors $2y^2+2yz+5z^2=117=10^2+4^2+1^2$, forme proposée.

*Autre exemple.* Le nombre 45 étant mis sous la forme $25+16+4$, le diviseur de $t^2+45u^2$ qui en résulte est

$$5y^2+10yz+14z^2=(2y+3z)^2+(y-z)^2+4z^2.$$

Soit $y=5$, $z=8$, on aura le diviseur particulier

$$1421=34^2+3^2+16^2.$$

Si d'après cette forme trinaire on cherche le diviseur de $t^2+1421u^2$, on trouvera

$$45y^2+34yz+38z^2=(4y+6z)^2+(5y-z)^2+(2y-z)^2,$$

dans lequel il est visible que 45 est compris. Et comme pour avoir 45, il faut faire $y=1$, $z=0$, la forme trinaire qui en résulte est

$$45=4^2+5^2+2^2,$$

la même que celle d'où on est parti. Ainsi on voit que quoique 45 et 1421 aient des facteurs quarrés et inégaux (car $1421=29.49$), la proposition est toujours vérifiée, et la forme trinaire $4^2+5^2+2^2$ est tellement liée avec la forme trinaire $34^2+16^2+3^2$, que l'une sert à faire retrouver l'autre.

(288) Théorème IX. *Si le diviseur quadratique* $py^2+2qyz+rz^2$ *relatif à la formule* $t^2+cu^2$, *est susceptible de plusieurs formes trinaires, et que dans ces diverses formes on substitue pour* y *et* z *les valeurs déterminées* $y=\alpha$, $z=\zeta$, *je dis que les formes trinaires qui en résulteront pour le nombre déterminé* $p\alpha^2+2q\alpha\zeta+r\zeta^2=N$, *seront différentes entr'elles, au moins tant que* N *surpassera* $\frac{4}{3}c$.

En effet, si l'on cherche par une analyse directe quels sont les cas où deux formes trinaires du diviseur $\Delta$, appliquées à un nombre particulier $N$, donnent une même valeur trinaire de ce nombre,

on trouvera que $N$ ne peut surpasser $\frac{2}{3}c$. C'est ce que nous allons développer avec l'étendue nécessaire.

Supposons que le diviseur quadratique $py^2+2qyz+rz^2=\Delta$ se décompose en trois quarrés de ces deux manières :

$$\Delta=(my+nz)^2+(m'y+n'z)^2+(m''y+n''z)^2$$
$$\Delta=(\mu y+\nu z)^2+(\mu' y+\nu' z)^2+(\mu'' y+\nu'' z)^2,$$

en sorte qu'on ait

$$p=m^2+m'^2+m''^2=\mu^2+\mu'^2+\mu''^2$$
$$q=mn+m'n'+m''n''=\mu\nu+\mu'\nu'+\mu''\nu''$$
$$r=n^2+n'^2+n''^2=\nu^2+\nu'^2+\nu''^2;$$

si les valeurs particulières de $y$ et de $z$ qui rendent le diviseur $\Delta$ égal à $N$ sont telles que les deux formes trinaires de $\Delta$ se réduisent à une seule de $N$, il faudra qu'on ait

$$\frac{y}{z}=\frac{\nu-n}{m-\mu}=\frac{\nu'-n'}{m'-\mu'}=\frac{\nu''-n''}{m''-\mu''}$$

(car on peut supposer alors que les trois quarrés composant les formes trinaires de $\Delta$ sont égaux terme à terme, et leurs racines de même signe).

Mais comme $y$ et $z$ doivent toujours être premiers entr'eux, il est clair que $\frac{y}{z}$ est l'expression la plus simple de ces fractions égales, et qu'ainsi en prenant trois nouvelles indéterminées $a, a', a''$, on pourra faire

$$m-\mu=az, \quad m'-\mu'=a'z, \quad m''-\mu''=a''z,$$
$$\nu-n=ay, \quad \nu'-n'=a'y, \quad \nu''-n''=a''y.$$

Tirant de ces équations les valeurs de $\mu, \nu, \mu', \nu', \mu'', \nu''$, et les substituant dans les quantités égales à $p, q, r$, on aura après les réductions,

$$\left.\begin{aligned}&\tfrac{1}{2}z(a^2+a'^2+a''^2)-ma-m'a'-m''a''=0\\&\tfrac{1}{2}y(a^2+a'^2+a''^2)+na+n'a'+n''a''=0\end{aligned}\right\}\ (\text{A})$$

$$\left.\begin{aligned}yz(a^2+a'^2+a''^2)+(na+n'a'+n''a'')z\\-(ma+m'a'+m''a'')y\end{aligned}\right\}=0,$$

où l'on voit que la troisième équation est une suite des deux autres, et qu'ainsi il suffit de satisfaire à celles-ci.

(289) De quelque manière qu'on satisfasse aux équations (A), les valeurs de $y$ et $z$ qui en résulteront, donneront un nombre $N = py^2 + 2qyz + rz^2$, tel que les deux formes trinaires du diviseur $\Delta$ se réduiront à une seule forme pour le nombre $N$. Il s'agit donc présentement de trouver la plus grande valeur de $N$ qui donne lieu à cette coincidence.

Observons d'abord que la somme $a^2 + a'^2 + a''^2$ ne peut être un nombre impair, car si elle en étoit un, les valeurs de $y$ et $z$ déduites des équations (A) seroient nécessairement des nombres pairs : ces valeurs ne seroient par conséquent pas admissibles, parce qu'on suppose toujours que $y$ et $z$ sont premiers entr'eux. On ne pourra donc faire $a = a' = a'' = 1$, et les plus simples valeurs qu'on puisse attribuer à ces quantités sont $a = 1$, $a' = 1$, $a'' = 2$. Nous commencerons par examiner cette hypothèse, laquelle, comme on le verra ensuite, est celle qui satisfait plus particulièrement à la question.

Cela posé, nous aurons les équations

$$p = m^2 + m'^2 + m''^2 \qquad N = py^2 + 2qyz + rz^2$$
$$q = mn + m'n' + m''n'' \qquad 3z = m + m' + 2m''$$
$$r = n^2 + n'^2 + n''^2 \qquad 3y = -n - n' - 2n'',$$

dans lesquelles il faut supposer $p$, $q$, $r$ donnés, et chercher les valeurs de $m$, $m'$, $m''$, $n$, $n'$, $n''$, telles que $y$ et $z$ soient les plus grandes possibles. Désignons par $\theta$ le rapport de $m''$ à $m'$ qui convient au *maximum* cherché, nous aurons $m'' = \theta m'$, $3z = m + (2\theta + 1)m'$, $p = m^2 + (1 + \theta^2)m'^2$. Si d'après ces deux équations on cherche le rapport de $m'$ à $m$ qui rend $z$ un *maximum*, on trouvera par les règles ordinaires $m' = \frac{m(2\theta+1)}{1+\theta^2}$, ce qui donnera

$$m = \sqrt{p} \cdot \frac{\sqrt{(1+\theta^2)}}{\sqrt{(2+4\theta+5\theta^2)}}, \quad z = \frac{\sqrt{p}}{3} \cdot \frac{\sqrt{(2+4\theta+5\theta^2)}}{\sqrt{(1+\theta^2)}}$$

$$m' = \sqrt{p} \cdot \frac{2\theta+1}{\sqrt{(1+\theta^2)} \cdot \sqrt{(2+4\theta+5\theta^2)}}$$

$$m'' = \sqrt{p} \cdot \frac{\theta \cdot (2\theta+1)}{\sqrt{(1+\theta^2)} \cdot \sqrt{(2+4\theta+5\theta^2)}}.$$

Les

Les rapports de $m$, $m'$, $m''$ étant substitués dans l'équation $q = mn + m'n' + m''n''$, il en résulte

$$\frac{q}{m'} = \theta n'' + n' + \frac{1+\theta^2}{2\theta+1} n.$$

Combinant cette équation où $q$, $m'$, $\theta$ sont censés donnés, avec les équations

$$r = n^2 + n'^2 + n''^2$$
$$3y = -n - n' - 2n'',$$

on trouvera que la condition $y = max.$ donne

$$n''\theta + n' = n(1+2\theta).$$

De-là résulte

$$q = n\sqrt{p} \cdot \frac{\sqrt{(2+4\theta+5\theta^2)}}{\sqrt{(1+\theta^2)}}$$
$$3y = (\theta-2)n'' - 2n(1+\theta)$$
$$r = (1+\theta^2)n''^2 - 2\theta(1+2\theta)nn'' + (2+4\theta+4\theta^2)n^2.$$

Ces trois équations donneront en éliminant $n''$ et $n$,

$$y = \frac{\sqrt{c}}{3\sqrt{p}} \cdot \frac{\theta-2}{\sqrt{(1+\theta^2)}} - \frac{q}{3p} \cdot \frac{\sqrt{(2+4\theta+5\theta^2)}}{\sqrt{(1+\theta^2)}}.$$

Et enfin si l'on substitue les valeurs trouvées de $y$ et $z$ dans l'équation $N = py^2 + 2qyz + rz^2$, on aura le *maximum* cherché $N = \tfrac{2}{3}c$, résultat qui, comme on voit, est indépendant de la valeur de $\theta$, ainsi que de celles de $p$, $q$ et $r$.

(290) Si, sans se conformer aux rapports qu'on vient de trouver, et qui le plus souvent seront irrationnels, on en approche jusqu'à un certain point, le nombre $N$ qui en résultera sera très-peu différent de $\tfrac{2}{3}c$.

Par exemple, le diviseur quadratiqne $251y^2 + 22yz + 617z^2$ qui appartient à la formule $t^2 + 154746u^2$, se décompose en trois quarrés de ces denx manières :

$$(5y-5z)^2 + (y-24z)^2 + (15y+4z)^2$$
$$(7y-2z)^2 + (11y+17z)^2 + (9y-18z)^2;$$

et si l'on fait $y = 7$, $z = 12$, ces deux formes trinaires se réduiront à une seule $25^2 + 281^2 + 153^2$ égale au nombre $102995 = N$: or on voit qu'en effet le nombre $N$ diffère très-peu de $\tfrac{2}{3}c$.

(291) Si on revient maintenant aux équations (A), et qu'on ne suppose plus aucune valenr particulière aux nombres $a, a', a''$, on trouvera par une analyse semblable, qne le plus grand nombre $N$ pour lequel les deux formes trinaires sont identiques, est généralement $N = \frac{4c}{a^2 + a'^2 + a''^2}$; ainsi si on supposoit $a = 1$, $a' = 2$, $a'' = 3$, on auroit $N = \frac{2}{7}c$. Et comme il faut toujours que $a^2 + a'^2 + a''^2$ soit un nombre pair (afin que $y$ et $z$ n'aient pas de commun diviseur), il s'ensuit que l'hypothèse qni donne le plus grand résultat possible, est celle que nons avons examinée en détail, et qui donne $N = \frac{2}{3}c$, conformément à l'énoncé du théorême.

(292) THÉORÈME X. *Si le nombre* N *est compris de* m *manières différentes dans un ou plusieurs diviseurs quadratiques de la formule* $t^2 + cu^2$; *si en outre chacun de ces diviseurs peut se décomposer en trois quarrés de* n *manières différentes, et qu'en conséquence le nombre* N *reçoive, comme diviseur de la formule* $t^2 + cu^2$, mn *valeurs trinaires, je dis que toutes ces formes trinaires seront différentes les unes des autres, excepté toutefois dans les cas où* N *étant plus petit que* $c^2$, *on pourroit satisfaire à l'équation* $c^2 = y^2 + Nz^2$.

En effet, l'une des formes trinaires de $N$ pent tonjours être représentée par la formule $N = \lambda^2 A^2 + \mu^2 B^2 + \nu^2 C^2$, en supposant que la valeur correspondante de $c$ soit $f^2\mu^2\nu^2 + g^2\nu^2\lambda^2 + h^2\lambda^2\mu^2$, et qu'on ait entre les nombres $A, B, C,$ la relation $fA + gB + hC = 0$.

Une seconde forme trinaire de $N$ pourra de même être représentée par la formnle $N = \lambda'^2 A'^2 + \mu'^2 B'^2 + \nu'^2 C'^2$, en supposant semblablement $c = f'^2\mu'^2\nu'^2 + g'^2\nu'^2\lambda'^2 + h'^2\lambda'^2\mu'^2$, et $f'A' + g'B' + h'C' = 0$.

Maintenant si l'on veut que ces deux valeurs trinaires de $N$ soient identiques, il faudra faire $\lambda A = \lambda' A'$, $\mu B = \mu' B'$, $\nu C = \nu' C'$. Tirant de ces équations les valeurs de $A'$, $B'$, $C'$, et les substituant dans l'équation $f'A' + g'B' + h'C' = 0$, on aura

$$f'\mu'\nu' . \lambda A + g'\nu'\lambda' . \mu B + h'\lambda'\mu' . \nu C = 0.$$

Celle-ci étant combinée avec l'équation $fA + gB + hC = 0$, il en résultera

$$\frac{\mu B}{\lambda A} = \frac{f'\mu'\nu' \cdot h\lambda\mu - h'\lambda'\mu' \cdot f\mu\nu}{h'\lambda'\mu' \cdot g\nu\lambda - g'\nu'\lambda' \cdot h\lambda\mu}$$
$$\frac{\nu C}{\lambda A} = \frac{g'\nu'\lambda' \cdot f\mu\nu - f'\mu'\nu' \cdot g\nu\lambda}{h'\lambda'\mu' \cdot g\nu\lambda - g'\nu'\lambda' \cdot h\lambda\mu}.$$

Soient pour abréger $f\mu\nu = \alpha$, $g\nu\lambda = \mathcal{C}$, $h\lambda\mu = \gamma$; $f'\mu'\nu' = \alpha'$, $g'\nu'\lambda' = \mathcal{C}'$, $h'\lambda'\mu' = \gamma'$, en sorte que les valeurs trinaires de $c$ qui répondent aux valeurs identiques de $N$, soient $c = \alpha^2 + \mathcal{C}^2 + \gamma^2$, $c' = \alpha'^2 + \mathcal{C}'^2 + \gamma'^2$, on aura

$$\frac{\mu B}{\lambda A} = \frac{\alpha'\gamma - \alpha\gamma'}{\gamma'\mathcal{C} - \gamma\mathcal{C}'}, \quad \frac{\nu C}{\lambda A} = \frac{\mathcal{C}'\alpha - \mathcal{C}\alpha'}{\gamma'\mathcal{C} - \gamma\mathcal{C}'}.$$

Mais les trois nombres $\lambda A$, $\mu B$, $\nu C$ ne peuvent être divisibles par un même facteur; donc si on appelle $\varphi$ le plus grand nombre qui puisse diviser à-la-fois les trois quantités $\alpha'\gamma - \alpha\gamma'$, $\mathcal{C}'\alpha - \mathcal{C}\alpha'$, $\gamma'\mathcal{C} - \gamma\mathcal{C}'$, on aura nécessairement

$$\varphi\lambda A = \gamma'\mathcal{C} - \gamma\mathcal{C}'$$
$$\varphi\mu B = \alpha'\gamma - \alpha\gamma'$$
$$\varphi\nu C = \mathcal{C}'\alpha - \mathcal{C}\alpha'.$$

De-là on déduit $\varphi^2(\lambda^2 A^2 + \mu^2 B^2 + \nu^2 C^2)$, ou $\varphi^2 N = (\gamma'\mathcal{C} - \gamma\mathcal{C}')^2 + (\alpha'\gamma - \alpha\gamma')^2 + (\mathcal{C}'\alpha - \mathcal{C}\alpha')^2$. Or, par une réduction qui se présente fréquemment dans ce genre d'analyse, on sait que le second membre de cette équation est la même chose que

$$(\alpha^2 + \mathcal{C}^2 + \gamma^2)(\alpha'^2 + \mathcal{C}'^2 + \gamma'^2) - (\alpha\alpha' + \mathcal{C}\mathcal{C}' + \gamma\gamma')^2;$$

de sorte que si l'on fait pour abréger $\alpha\alpha' + \mathcal{C}\mathcal{C}' + \gamma\gamma' = \theta$, on aura $\varphi^2 N = c^2 - \theta^2$, ou $c^2 = \theta^2 + N\varphi^2$.

Donc deux formes trinaires ne sauroient être identiques, à moins que le nombre $N$ ne soit plus petit que $c^2$, et tel qu'on puisse satisfaire à l'équation $c^2 = y^2 + Nz^2$.

Donc si $N$ est plus grand que $c^2$, ou si $N$, sans être plus grand que $c^2$, est tel que l'équation $c^2 = y^2 + Nz^2$ soit impossible, toutes les valeurs trinaires de $N$, déduites des diverses formes des diviseurs trinaires de la formule $t^2 + cu^2$, seront différentes les unes des autres.

(293) On a déjà prouvé (n°. 243) que s'il y a $i$ nombres premiers différens qui divisent $N$ ou $\frac{1}{2}N$ sans diviser $c$, il y aura $2^{i-1}$ manières de satisfaire à l'équation $N = py^2 + 2qyz + rz^2$, ou aux

équations semblables dont le second membre est un diviseur quadratique de la formule $t^2+cu^2$. Donc si chacun de ces diviseurs quadratiques se décompose de $K$ manières en trois quarrés, et qu'en outre l'équation $c^2=y^2+Nz^2$ ne puisse avoir lieu, il faudra que le nombre $N$ reçoive, comme diviseur de la formule $t^2+cu^2$, $K.2^{i-1}$ formes trinaires différentes. Multiplicité qui, comme on voit, peut être fort considérable, et qui cependant pourra ne faire qu'une partie de toutes les formes trinaires dont $N$ est susceptible.

Pour confirmer ce résultat par un exemple, considérons la formule $t^2+21u^2$, et son diviseur quadratique $5y^2+6yz+6z^2$, lequel est susceptible de deux formes trinaires, savoir :

$$5y^2+6yz+6z^2=\begin{cases}(2y+z)^2+(y+z)^2+4z^2\\(y-z)^2+(2y+2z)^2+z^2.\end{cases}$$

Dans ce diviseur est compris le nombre 17765, composé de quatre facteurs 5 . 11 . 17 . 19 ; et parce que 17765 est de la forme $84x+41$, on trouve aisément à l'inspection de la Table IV, que ce nombre ne peut être contenu que dans la formule $5y^2+6yz+6z^2$; il doit d'ailleurs y être contenu de huit manières, puisqu'étant formé de quatre facteurs, non diviseurs de $c$, on a $i=4$, et $2^{i-1}=2^3=8$. En effet, si on résout l'équation $17765=5y^2+6yz+6z^2$ ou $88825=(5y+3z)^2+21z^2$, on trouvera ces huit solutions :

$$\begin{array}{l}y=59,\ 49,\ -67,\ 41,\ 37,\ -71,\ 23,\ 13\\z=\ 1,\ 15,\ \ 15,\ 24,\ 28,\ \ 31,\ 40,\ 47.\end{array}$$

On en trouveroit même huit autres, mais qui ne produiroient aucun nouveau résultat, parce qu'on doit regarder la solution $y=\alpha$, $z=\zeta$, et la solution $y=\alpha$, $z=-\alpha-\zeta$, comme n'en faisant qu'une. Cela posé, les huit solutions trouvées donneront chacune deux formes trinaires de 17765; et par conséquent ce nombre, comme diviseur de $t^2+21u^2$, aura les seize formes trinaires suivantes, toutes différentes les unes des autres :

| | | | |
|---|---|---|---|
| $119^2+60^2+2^2$ | $119^2+52^2+30^2$ | $102^2+65^2+56^2$ | $86^2+63^2+80^2$ |
| $58^2+120^2+1^2$ | $82^2+104^2+15^2$ | $9^2+130^2+28^2$ | $17^2+126^2+40^2$ |
| $113^2+64^2+30^2$ | $106^2+65^2+48^2$ | $111^2+40^2+62^2$ | $73^2+60^2+94^2$ |
| $34^2+128^2+15^2$ | $17^2+130^2+24^2$ | $102^2+80^2+31^2$ | $34^2+120^2+47^2$ |

*Remarque.* Si $N$ est pair et plus grand que $\frac{1}{4}c^2$, l'équation $c^2 = \theta^2 + N\varphi^2$ ne pourra avoir lieu, et la proposition générale ne sera point sujette à exception.

En effet, dans ce cas, la valeur de $\varphi$ ne peut être que 1, et ainsi on auroit $N = c^2 - \theta^2$; mais $N$ étant pair, il faudra que les nombres $c$ et $\theta$ soient tous deux pairs ou tous deux impairs, et dans les deux cas, $c^2 - \theta^2$ seroit divisible par 4, tandis que le nombre $N$, comme compris dans un diviseur quadratique, ne peut être que le double d'un impair. Donc il est impossible alors que l'équation $N = c^2 - \theta^2$ ait lieu, donc toutes les formes trinaires de $N$ déduites des diviseurs de la formule $t^2 + cu^2$, seront différentes entr'elles.

Dans la même supposition de $N > \frac{1}{4}c^2$, l'équation $N = c^2 - \theta^2$ ne pourra encore avoir lieu, si $N$ étant de la forme $4n+1$, $c$ est pair, ou si $N$ étant de la forme $8n+3$, $c$ est impair. Donc dans tous ces cas, qui sont fort étendus, la proposition générale ne sera sujette à aucune exception, et toutes les formes trinaires de $N$ seront différentes entr'elles.

## §. V. *Explication des Tables VIII, IX, X et XI.*

### TABLE VIII.

(294) Cette Table contient les diviseurs quadratiques $4n+1$ de la formule $t^2+cu^2$, pour tout nombre $c$ de forme $4n+1$ depuis $c=1$ jusqu'à $c=213$, sans excepter les nombres quarrés ni les nombres divisibles par des quarrés.

Chaque diviseur quadratique, dans son expression ordinaire, est mis sous la forme $py^2+2qyz+2mz^2$, laquelle, comme nous l'avons déjà remarqué, a l'avantage d'en faire connoître une autre $2py^2+2qyz+mz^2$. Mais celle-ci n'appartient aux diviseurs $4n+1$, les seuls qui soient compris dans la Table, que lorsque $c$ est de forme $8n+1$.

L'objet principal qu'on s'est proposé dans cette Table, est de développer les diverses formes trinaires dont chaque diviseur quadratique est susceptible, et de montrer la correspondance de ces décompositions avec les diverses formes trinaires du nombre $c$, lesquelles sont placées dans la première colonne à gauche.

Dans cette disposition, on a été conduit à distinguer trois espèces différentes parmi les diviseurs quadratiques $4n+1$ de la formule $t^2+cu^2$.

(295) Le diviseur quadratique $py^2+2qyz+rz^2$ appartient à la *première espèce*, s'il est décomposable en trois quarrés, et si parmi les formes trinaires dont il est susceptible, il y en a au moins une $(my+nz)^2+(m'y+n'z)^2+(m''y+n''z)^2$ telle que la valeur correspondante de $c$, savoir $c=(mn'-m'n)^2+(m'n''-m''n')^2+(m''n-mn'')^2$, n'ait pas ses trois termes divisibles par un même quarré.

La seconde condition aura lieu nécessairement, lorsque le nombre $c$ n'a aucun facteur quarré; ainsi dans ce cas tout diviseur quadratique trinaire est de première espèce.

Mais lorsque le nombre $c$ est divisible par un quarré, le diviseur $py^2+2qyz+rz^2$ pourra être trinaire ou décomposable en trois

quarrés, sans satisfaire à la condition mentionnée, et alors il ne sera pas de première espèce. C'est ainsi que le diviseur quadratique $13y^2+18yz+18z^2$ de la formule $t^2+153u^2$, quoiqu'il se décompose en trois quarrés $4y^2+9z^2+9(y+z)^2$, n'est cependant pas de la première espèce, par deux raisons, 1°. parce que la valeur de $c$ qui résulte de cette décomposition, savoir $c=81+36+36$, a ses trois termes divisibles par 9; 2°. parce que ce diviseur n'est susceptible d'aucune autre décomposition ou forme trinaire; de sorte qu'il n'est pas possible de lui donner une forme qui ait la condition requise pour la première espèce.

La même formule $t^2+153u^2$ offre un autre diviseur quadratique $2y^2+2yz+77z^2$, qu'on peut mettre sous la forme $(y+5z)^2+(y-4z)^2+36z^2$; d'où résulte encore $c=81+36+36$, valeur qui ne convient pas à la première espèce; mais ce même diviseur peut aussi se décomposer en ces trois quarrés $(y+3z)^2+(y-2z)^2+64z^2$, d'où résulte $c=64+64+25$, valeur dont les trois termes ne sont pas divisibles par un même nombre. Donc le diviseur quadratique $2y^2+2yz+77z^2$ appartient à la première espèce.

Les diviseurs quadratiques *de la seconde espèce* sont ceux qu'on ne peut décomposer en trois quarrés, et qui par cette raison sont marqués dans les Tables *non décomposables*. Tels sont le diviseur $y^2+2yz+34z^2$ pour la formule $t^2+33u^2$, le diviseur $18y^2+10yz+5z^2$ pour la formule $t^2+65u^2$, et une infinité d'autres.

Enfin les diviseurs quadratiques *de la troisième espèce* sont ceux qui peuvent bien être décomposés en trois quarrés, mais dont toutes les formes trinaires sont telles que les valeurs correspondantes de $c$ ont chacune les trois termes divisibles par un même quarré; d'où l'on voit que tout diviseur trinaire qui n'est pas de la première espèce sera nécessairement de la troisième; ainsi le diviseur $13y^2+18yz+18z^2$, dont nous avons fait déjà mention, appartient à la troisième espèce.

(296) Nous avons compris dans une même colonne les diviseurs de la première, deuxième et troisième espèces. On peut cependant distinguer au premier coup-d'œil les trois espèces; savoir, la première, en ce que les diviseurs qui lui appartiennent sont au premier

rang, qu'ils sont actuellement décomposés en trois quarrés, que chaque décomposition répond à une valeur trinaire du nombre $c$, et que parmi ces valeurs, placées dans la première colonne, il y en a toujours au moins une dont les trois termes ne sont pas divisibles par un même nombre.

La seconde espèce se reconnoît immédiatement, en ce qu'elle n'est point décomposée en quarrés, et qu'elle ne répond à aucune forme trinaire de $c$. On a ajouté à chaque diviseur de cette espèce l'expression *non décomposable* qui le caractérise.

La troisième espèce, quand il y a lieu, vient à la suite de la première ou des deux premières : elle est séparée de celles-ci par un trait, et distinguée par un caractère d'impression différent. On remarquera aussi que les trois quarrés composant la valeur correspondante de $c$ ont toujours un commun diviseur. Dans cette troisième espèce, la décomposition en trois quarrés est souvent possible de plusieurs manières, mais nous nous sommes contentés d'indiquer une décomposition.

Il est inutile d'observer que cette troisième espèce ne peut avoir lieu que lorsque $c$ est divisible par un quarré. Si on eût omis, comme il a été pratiqué dans les Tables générales des diviseurs quadratiques et linéaires, toutes les formules où $c$ est quarré ou divisible par un quarré, on n'auroit point rencontré cette troisième espèce de diviseurs quadratiques. Il a été nécessaire cependant de comprendre ces formules avec les autres, parce que la suppression de ces intermédiaires auroit nui à l'enchaînement des propositions, et rendu plus difficiles leurs démonstrations.

Remarquons que les trois espèces dans lesquelles nous avons distingué les diviseurs quadratiques $4n+1$, s'excluent mutuellement, et renferment cependant tous les cas possibles ; de sorte que tout diviseur quadratique $4n+1$ appartient nécessairement à l'une des trois espèces, et ne peut appartenir qu'à une seule.

(297) Voici maintenant diverses propriétés générales qui se présentent à l'inspection de la Table, et qu'on observeroit également si la Table étoit prolongée beaucoup plus loin.

1°. Quel que soit le nombre $c$ de forme $4n+1$, il existe toujours

jours un ou plusieurs diviseurs de première espèce pour la formule $t^2+cu^2$, ce qui suppose que tout nombre $4n+1$ est décomposable en trois quarrés, et que de plus il y a une décomposition telle, que les trois quarrés n'ont pas de diviseur commun.

2°. Lorsque le nombre $c$ est premier, tous les diviseurs quadratiques $4n+1$ de la formule $t^2+cu^2$ sont de la première espèce et par conséquent de forme trinaire. Chacun d'eux répond à une valeur trinaire de $c$, différente pour les différens diviseurs.

3°. Lorsque le nombre $c$ est divisible par un quarré, la formule $t^2+cu^2$ a toujours un ou plusieurs diviseurs quadratiques de troisième espèce, et dans ce même cas, elle peut en avoir aussi de la seconde. On en voit un exemple à l'égard des diviseurs de la formule $t^2+117u^2$.

4°. Lorsque le nombre $c$ est composé de facteurs premiers inégaux, la formule $t^2+cu^2$ a toujours un ou plusieurs diviseurs quadratiques de la seconde espèce, c'est-à-dire, non décomposables en trois quarrés.

5°. Lorsque $c$ est un nombre premier, les diviseurs quadratiques qui sont tous trinaires, ne le sont chacun que d'une seule manière, conformément à la proposition du n°. 284. Mais lorsque $c$ est un nombre composé, chaque diviseur quadratique de la première espèce est autant de fois trinaire ou décomposable en trois quarrés, qu'il y a de manières de former $c$ du produit de deux facteurs.

## TABLE IX.

(298) La Table IX renferme les diviseurs quadratiques $4n+2$ de la formule $t^2+cu^2$, pour tout nombre $c$ de forme $8n+3$, depuis $c=3$ jusqu'à $c=219$. Les diviseurs sont réduits à la forme $2py^2+2qyz+2rz^2$, où l'on a $p$, $q$, $r$ impairs, $q<p$ et $r$, et $4pr-q^2=c$.

On distingue encore ici trois espèces de diviseurs. La première est toujours décomposable en trois quarrés, auxquels répond une valeur de $c$ exprimée en trois quarrés impairs qui n'ont pas de commun diviseur.

La seconde espèce n'est point décomposable en trois quarrés, et ne répond par conséquent à aucune forme trinaire du nombre $c$.

Enfin la troisième espèce est décomposable, mais les trois quarrés qui en résultent pour la valeur correspondante de $c$ ont toujours un commun diviseur. Et ainsi cette troisième espèce ne peut avoir lieu que lorsque le nombre $c$ est divisible par un quarré.

(299) Voici maintenant les remarques que présentent les diviseurs selon la nature du nombre $c$.

1°. Lorsque le nombre $c$ est premier, les diviseurs quadratiques $4n+2$ sont tous de la première espèce, et de plus, chaque diviseur n'est décomposable en trois quarrés que d'une seule manière.

2°. Lorsque le nombre $c$ est composé, et qu'il n'a que des facteurs simples, comme 35, 51, 91, &c., il y a toujours un ou plusieurs diviseurs de la seconde espèce; il ne peut y en avoir de la troisième.

3°. Lorsque le nombre $c$ est divisible par un quarré, il y a toujours un ou plusieurs diviseurs de la troisième espèce. Il peut y en avoir en même temps de la seconde.

4°. Dans tous les cas, il y a des diviseurs de la première espèce, ce qui suppose que tout nombre $8n+3$ est la somme de trois quarrés, conformément au théorême de Fermat (n°. 155); mais on voit, de plus, que la décomposition en trois quarrés peut toujours être faite de manière que ces trois quarrés n'aient pas de commun diviseur.

5°. Lorsque $c$ est un nombre composé, tout diviseur quadratique de première espèce se développe en autant de formes trinaires qu'il y a de manières de former $c$ du produit de deux facteurs.

Dans cette Table, ainsi que dans la précédente, les diviseurs trinaires de la première espèce sont développés en trois quarrés de toutes les manières possibles, et on a mis en même temps, vis-à-vis de chaque forme trinaire du diviseur, la forme trinaire correspondante de $c$. Quant aux diviseurs de la troisième espèce, on a indiqué seulement une de leurs formes trinaires.

## TABLE X.

(300) Cette Table contient les diviseurs quadratiques $8n+1$ et $8n+3$ de la formule $t^2+2au^2$, $a$ étant un nombre de la forme

$4n+1$ ; elle est calculée pour toutes les valeurs de $a$ depuis $a=1$ jusqu'à $a=117$.

Chaque diviseur quadratique est représenté par la formule $py^2+2qyz+2mz^2$ dans laquelle $q$ est pair, $p$ et $m$ impairs et $q<p$ et $m$. Cette forme est toujours accompagnée de sa conjuguée $2py^2+2qyz+mz^2$, mais celle-ci ne se trouve parmi les diviseurs $8n+1$, $8n+3$, que lorsque $a$ est de la forme $8n+1$.

On distingue les diviseurs compris dans cette Table en trois espèces analogues à celles des deux Tables précédentes, et ces diverses sortes donnent lieu aux propriétés suivantes.

1°. Lorsque le nombre $a$ est premier, les diviseurs quadratiques $8n+1$, $8n+3$ sont toujours de la première espèce, et il n'y en a aucun de la seconde.

Dans ce même cas, chaque diviseur se décompose en trois quarrés d'une manière seulement, et ne répond non plus qu'à une seule forme trinaire du nombre $2a$.

2°. Lorsque le nombre $a$ est composé, et qu'il n'a que des facteurs simples, il existe toujours un ou plusieurs diviseurs quadratiques de la seconde espèce.

3°. Lorsque $a$ est divisible par un quarré, il existe toujours un ou plusieurs diviseurs quadratiques de la troisième espèce. Il peut aussi y en avoir de la seconde espèce.

4°. Quel que soit le nombre $a$, il existe toujours un ou plusieurs diviseurs quadratiques de la première espèce, ce qui suppose que tout nombre $8n+2$ est la somme de trois quarrés, et, de plus, qu'on peut faire la décomposition de manière que les trois quarrés ne soient pas divisibles par un même nombre.

5°. Lorsque $a$ est un nombre composé, chaque diviseur de la première espèce prend autant de formes trinaires qu'il y a de manières de former $a$ du produit de deux facteurs.

Dans cette Table, comme dans les deux précédentes, on a mis toutes les formes trinaires de $2a$ qui répondent aux diviseurs trinaires. Les diviseurs trinaires eux-mêmes sont développés dans toutes leurs formes possibles, lorsqu'ils sont de la première espèce; quant à ceux de la troisième espèce, on en a indiqué seulement une décomposition.

## TABLE XI.

(301) Cette Table contient les diviseurs quadratiques $8n+3$, $8n+5$ de la formule $t^2+2au^2$, $a$ étant de la forme $4n-1$. Elle est calculée pour toutes les valeurs de $a$ depuis $a=3$ jusqu'à $a=123$.

Ces diviseurs se distinguent en trois espèces comme ceux des Tables précédentes. Ils offrent semblablement les propriétés suivantes.

1°. Lorsque $a$ est un nombre premier, les diviseurs quadratiques $8n+3$, $8n+5$, sont tous de la première espèce, et il n'y en a aucun de la seconde.

De plus, chaque diviseur ne se décompose en trois quarrés que d'une seule manière, et ne répond non plus qu'à une seule forme trinaire du nombre $2a$.

2°. Lorsque le nombre $a$ est composé, et qu'il n'a que des facteurs simples, il y a toujours un ou plusieurs diviseurs quadratiques de la seconde espèce.

3°. Lorsque le nombre $a$ est divisible par un quarré, il y a toujours un ou plusieurs diviseurs de la troisième espèce.

4°. Quel que soit le nombre $a$ de forme $4n-1$, il existe toujours un ou plusieurs diviseurs quadratiques de la première espèce, ce qui suppose que tout nombre $8n-2$ est la somme de trois quarrés non-divisibles par un même facteur.

5°. Lorsque le nombre $a$ est composé, chaque diviseur de première espèce peut se développer en autant de formes trinaires qu'il y a de manières de former $a$ du produit de deux facteurs.

Ces formes sont toutes indiquées dans la Table, ainsi que les valeurs trinaires correspondantes de $2a$. A l'égard des diviseurs de troisième espèce, on n'a indiqué qu'une de leurs formes trinaires, quoiqu'ils puissent quelquefois en avoir plusieurs.

*Remarque.* On pourroit réunir en une seule Table, suivant l'ordre des nombres $c$, tous les diviseurs de première espèce contenus dans les Tables VIII, IX, X et XI; mais alors il seroit bon d'omettre celles des formes trinaires des diviseurs, dans lesquelles la valeur correspondante de $c$ a ses trois termes divisibles par un

même quarré, attendu que ces formes n'appartiennent qu'improprement, ou même sont étrangères aux diviseurs de la première espèce. Par cette disposition, l'enchaînement des différentes formules exprimé par le théorême VIII deviendroit plus sensible, et le nombre des formes trinaires de chaque diviseur quadratique seroit en général $2^{i-1}$, $i$ étant le nombre de facteurs premiers, impairs et inégaux qui divisent $c$.

Dans la Table ainsi formée, on observera encore que tous les diviseurs quadratiques d'une même formule $t^2+cu^2$, répondent à un même groupe de diviseurs linéaires. Or suivant une propriété des diviseurs de première espèce qui sera démontrée ci-après, si $N$ est un nombre quelconque compris dans ces diviseurs, il faut réciproquement que $c$ soit diviseur de $t^2+Nu^2$. De-là il est facile de trouver *a priori* les formes linéaires des diviseurs de première espèce; pour cela soient $\alpha$, $\beta$, $\gamma$, &c. les nombres premiers, inégaux et impairs, qui divisent $c$, il faudra d'abord satisfaire aux équations $\left(\frac{-N}{\alpha}\right)=1$, $\left(\frac{-N}{\beta}\right)=1$, $\left(\frac{-N}{\gamma}\right)=1$, &c. Ensuite, par la combinaison des solutions, on obtiendra toutes les formes linéaires cherchées; et il sera bon de réunir dans ces formes linéaires, non-seulement tous les diviseurs impairs, comme on l'a fait jusqu'à présent, mais aussi tous les diviseurs doubles d'un impair. (Voyez ci-après, n°. 305.)

---

## §. VI. THÉORÈMES comprenant la démonstration des propriétés observées dans les Tables.

(302) THÉORÈME XI. *Soit* $py^2+2qyz+rz^2$ *un diviseur quadratique de la formule* $t^2+cu^2$, *et soient* p *et* c *premiers entr'eux ; si l'on suppose que* c *est diviseur de* $t^2+pu^2$, *je dis que* c *sera diviseur de* $t^2+Nu^2$, N *étant un nombre quelconque renfermé dans la formule* $py^2+2qyz+rz^2$.

En effet, soit $N=p\alpha^2+2q\alpha\mathcal{C}+r\mathcal{C}^2$, on aura $pN=(p\alpha+q\mathcal{C})^2+c\mathcal{C}^2$. Mais par hypothèse, $c$ est diviseur de $t^2+pu^2$, donc il existe un entier $k$, tel que $\frac{k^2+p}{c}$ est un entier. Donc $\frac{Nk^2+Np}{c}$ sera aussi un entier: mettant au lieu de $pN$ sa valeur, on aura $\frac{(p\alpha+q\mathcal{C})^2+Nk^2}{c}=e$. Or $c$ et $k$ sont premiers entr'eux ; car s'ils avoient un commun diviseur $\theta$, l'expression $\frac{k^2+p}{c}$ étant un entier, il faudroit que $p$ et $c$ eussent le même commun diviseur $\theta$, ce qui est contre la supposition. Donc on peut faire $p\alpha+q\mathcal{C}=kx+cu$, et on aura $\frac{x^2+N}{c}=e$. Donc $c$ est diviseur de $x^2+N$, ou en général de la formule $t^2+Nu^2$.

*Remarque.* La même proposition aura lieu, en supposant seulement que le diviseur quadratique $py^2+2qyz+rz^2$ renferme un nombre $p'$ premier à $c$, et tel que $c$ soit diviseur de $t^2+p'u^2$. Car on pourra toujours, par une transformation, faire en sorte que ce nombre $p'$ tienne la place du premier coefficient $p$ (n°. 231).

Donc si un seul nombre $p'$ premier à $c$, et contenu dans le diviseur quadratique $py^2+2qyz+rz^2$, est tel que $c$ soit diviseur de $t^2+p'u^2$, tout nombre $N$ compris dans ce même diviseur quadratique jouira de la même propriété ; de sorte que $c$ sera toujours diviseur de la formule $t^2+Nu^2$.

(303) Théorème XII. *Au contraire, si un seul nombre* p′ *renfermé dans le diviseur quadratique* $py^2+2qyz+rz^2$ *est tel que* c *ne divise pas* $t^2+p'u^2$, *je dis que tout nombre* N *renfermé dans le même diviseur est tel aussi que* c *n'est pas diviseur de* $t^2+Nu^2$, *au moins en supposant* N *et* c *premiers entr'eux.*

Car puisque $c$ et $N$ sont premiers entr'eux, si $c$ divisoit $t^2+Nu^2$, il faudroit, en vertu du théorème précédent, que $c$ divisât aussi $t^2+p'u^2$, ce qui est contre la supposition.

(304) Nous appellerons, pour abréger, *diviseur réciproque* tout diviseur quadratique de la formule $t^2+cu^2$, dont la propriété est telle, que $N$ étant un nombre quelconque compris dans ce diviseur, réciproquement $c$ soit diviseur de $t^2+Nu^2$.

Nous appellerons par opposition *diviseur non réciproque*, tout diviseur quadratique qui ne jouit pas de cette propriété, ou qui n'en jouit que par rapport à quelques nombres particuliers $N$ qui ont un commun diviseur avec $c$.

Les conditions pour qu'un divisenr quadratique soit réciproque ou ne le soit pas, sont tellement précisées par les deux théorêmes précédens, qu'on pourra toujours décider promptement, et presque à la seule inspection, si un diviseur quadratique donné est réciproque ou non.

Prenons pour exemple la formule $t^2+69u^2$ et son diviseur quadratique $5y^2+2yz+14z^2$ : pour savoir si ce diviseur est réciproque, j'observe que le coefficient 5 est premier à 69; je cherche donc si 69 est diviseur de $t^2+5u^2$. Or il est manifeste que 69 divise $8^2+5$; donc le diviseur quadratique dont il s'agit est un diviseur réciproque; c'est-à-dire que si $N$ est un nombre quelconque compris dans $5y^2+2yz+14z^2$, on peut être assuré que 69 est diviseur de $t^2+Nu^2$.

La même formule $t^2+69u^2$ ayant un autre diviseur quadratique $13y^2+6yz+6z^2$, pour savoir si celui-ci est réciproque, je cherche si 69 est diviseur de $t^2+13u^2$. Or on voit immédiatement que 3 n'est point diviseur de $t^2+13u^2$; donc à plus forte raison 69 ne peut l'être; donc le diviseur quadratiqne $13y^2+6yz+6z^2$ est un diviseur non réciproque.

Considérons encore la formule $t^2+45u^2$ et son diviseur quadratique $y^2+2yz+46z^2$. Pour déterminer la nature de ce diviseur, je prends le coefficient 1 du premier terme, et je cherche si 45 divise $t^2+1u^2$. Mais on voit tout de suite que 3 ne divise point $t^2+u^2$, donc 45 ne peut le diviser (car on suppose toujours $t$ et $u$ premiers entr'eux). Donc le diviseur dont il s'agit est un diviseur non réciproque.

REMARQUE.

(305) *Les propriétés contenues dans ces deux théorèmes, et celles qui font le sujet de tout ce paragraphe, ne concernent pas tous les diviseurs quadratiques de la formule* $t^2+cu^2$, *mais seulement ceux qui sont de nature à entrer dans les Tables VIII, IX, X et XI. Sur quoi il faut se rappeler,*

1°. Que la Table VIII, lorsque $c=8n+1$, contient les diviseurs $4n+1$, et les diviseurs $8n+2$ de la formule $t^2+cu^2$.

2°. Que la même Table VIII, lorsque $c=8n+5$, contient les diviseurs $4n+1$ et les diviseurs $8n+6$ de la formule $t^2+cu^2$.

3°. Que la Table IX, où $c=8n+3$, contient généralement tous les diviseurs $4n+2$ de la formule $t^2+cu^2$.

4°. Que la Table X, où $c=8n+2$, contient les diviseurs $8n+1$, $8n+3$, et les diviseurs $16n+10$, $16n+14$ de la formule $t^2+cu^2$.

5°. Que la Table XI, où $c=8n+6$, contient les diviseurs $8n+3$, $8n+5$, et les diviseurs $16n+2$, $16n+14$ de la formule $t^2+cu^2$.

Ces Tables n'offrent, ni dans les nombres $c$, ni dans les diviseurs particuliers de la formule $t^2+cu^2$, aucun nombre divisible par 4, ni aucun nombre $8n+7$.

(306) THÉORÈME XIII. *Si le nombre* c *est premier ou double d'un premier, tout diviseur quadratique de la formule* $t^2+cu^2$ *sera un diviseur réciproque.* (On ne parle ici que des diviseurs compris dans les Tables VIII, IX, X et XI).

Il y a quatre cas à examiner, selon que le nombre $c$ se rapporte à l'une des quatre Tables citées.

1°. Si $c$ est un nombre premier de forme $4n+1$, il a déjà été démontré

démontré (n°. 196) que $N$ étant un diviseur quelconque $4n+1$ de la formule $t^2+cu^2$, on a $\left(\frac{N}{c}\right)=1$ ; donc $c$ est diviseur de $t^2+Nu^2$. Donc le diviseur quadratique qui renferme $N$ est un diviseur réciproque.

2°. Si $c$ est un nombre premier $8n+3$, et $P$ un diviseur quelconque impair de la formule $t^2+cu^2$, on aura (n°. 197) $\left(\frac{P}{c}\right)=1$. On a en même temps, par la nature du nombre $c$ (n°. 148), $\left(\frac{2}{c}\right)=-1$ ; donc $\left(\frac{2P}{c}\right)=-1$ ; donc $c$ est diviseur de $t^2+2Pu^2$ ou de $t^2+Nu^2$, $N$ étant un diviseur quelconque $4n+2$ de la formule $t^2+cu^2$. Donc tout diviseur quadratique $4n+2$ de cette formule est un diviseur réciproqne.

3°. Si le nombre $c=2a$, $a$ étant un nombre premier $4n+1$, il a été déjà démontré, n°. 198, qu'on a $\left(\frac{N}{c}\right)=1$, $N$ étant un diviseur quelconque $8n+1$ ou $8n+3$ de la formule $t^2+cu^2$ ou $t^2+2au^2$. Donc $a$ est diviseur de $t^2+Nu^2$ ; donc $2a$ ou $c$ l'est aussi. Donc le diviseur quadratique qui renferme $N$ est un diviseur réciproque.

4°. Si le nombre $c=2a$, $a$ étant uu nombre premier $4n-1$, on a prouvé, n°. 198, que $N$ étant nn diviseur quelconque $8n+3$ ou $8n+5$ de la formule $t^2+2au^2$, on a $\left(\frac{N}{a}\right)=-1$. Donc $a$ est diviseur de la formule $t^2+Nu^2$ ; donc $2a$ ou $c$ l'est aussi. Donc le diviseur quadratiqne qui renferme $N$ est un diviseur réciproque.

(307) THÉORÈME XIV. *Si le nombre c ou sa moitié est un nombre composé, la formule* $t^2+cu^2$ *aura toujours au moins un diviseur quadratique réciproque ; elle aura aussi au moins un diviseur quadratique non-réciproque.*

Nous nons contenterons de démontrer cette proposition pour la Table VIII, attendu que le raisonnement est le même pour les autres Tables.

Soit donc $c$ un nombre composé $4n+1$, si l'on peut prouver

qu'il existe un nombre premier $N$ également de forme $4n+1$, tel que $c$ soit diviseur de $t^2+Nu^2$, il s'ensuivra (n°. 196) que $\left(\frac{c}{N}\right)=1$ ou que $N$ est diviseur de $t^2+cu^2$, et qu'ainsi le diviseur quadratique qui contient $N$ est un diviseur réciproque, ce qui est la première partie du théorême.

Pour cet effet, décomposons $c$ en ses facteurs premiers égaux ou inégaux : soient $\alpha, \alpha', \alpha''$, &c. les facteurs $4n+1$, et $\mathcal{C}, \mathcal{C}', \mathcal{C}''$, &c. les facteurs $4n-1$, ceux-ci étant en nombre pair, puisque $c$ est de forme $4n+1$. On aura donc $c=\alpha\alpha'\alpha''\ldots\mathcal{C}\mathcal{C}'\mathcal{C}''\mathcal{C}'''$; et pour que $c$ divise la formule $t^2+Nu^2$, il faut qu'on ait les diverses égalités conditionnelles

$$\left(\frac{N}{\alpha}\right)=1, \quad \left(\frac{N}{\alpha'}\right)=1, \quad \left(\frac{N}{\alpha''}\right)=1, \quad \text{\&c.}$$

$$\left(\frac{N}{\mathcal{C}}\right)=-1, \quad \left(\frac{N}{\mathcal{C}'}\right)=-1, \quad \left(\frac{N}{\mathcal{C}''}\right)=-1, \quad \text{\&c.}$$

Or chacune de ces conditions (rapportée à un dénominateur différent) fournit en général plusieurs valeurs linéaires de $N$ (n°. 193), et ces valeurs étant combinées entr'elles, pour satisfaire à toutes les équations, donneront un grand nombre de formules dont chacune contient une infinité de nombres premiers; il n'y a donc aucun lieu de douter qu'on ne puisse trouver un nombre premier $N$ qui satisfasse à la condition requise; et ce nombre premier $N$ déterminera à lui seul (n°. 232) un diviseur quadratique de la formule $t^2+cu^2$, lequel sera réciproque (n°. 304), puisque $c$ divise $t^2+Nu^2$.

Venons maintenant à la seconde partie du théorême, et prouvons que la formule $t^2+cu^2$ a aussi un diviseur quadratique $4n+1$ non réciproque.

Soit $c=c'\theta$, $\theta$ étant un nombre premier que nous supposerons d'abord de forme $4n+1$. On cherchera (1) un nombre premier $N$

(1) Pour faire voir comment on peut trouver la forme générale des nombres $N$ qui satisfont à ces conditions, prenons un cas particulier, et supposons que $c'$ est composé du produit de trois facteurs premiers $\alpha\mathcal{C}\gamma$; la condition $\left(\frac{\alpha\mathcal{C}\gamma}{N}\right)=-1$ pourra être remplie de plusieurs manières. Par exemple, on pourra supposer

de la même forme $4n+1$, tel qu'on ait à-la-fois $\left(\frac{c'}{N}\right)=-1$, $\left(\frac{\theta}{N}\right)=-1$. Le nombre ainsi trouvé, $N$ sera diviseur de la formule $t^2+cu^2$, puisqu'on aura $\left(\frac{c}{N}\right)=\left(\frac{c'\theta}{N}\right)=1$; mais la propriété réciproque n'aura pas lieu; car ayant $\left(\frac{\theta}{N}\right)=-1$, il s'ensuit que $\left(\frac{N}{\theta}\right)=-1$; donc $\theta$ n'est pas diviseur de $t^2+Nu^2$, ni à plus forte raison $c'\theta$ ou $c$. Il existe donc un nombre premier $N$ de forme $4n+1$ qui divise $t^2+cu^2$, sans que réciproquement $c$ divise $t^2+Nu^2$, et ainsi $N$ doit être contenu dans un diviseur quadratique non réciproque de la formule $t^2+cu^2$.

S'il n'y avoit aucun nombre premier de forme $4n+1$ qui divisât $c$, alors il faudroit supposer $\theta$ de forme $4n-1$. Dans ce cas, on chercheroit le nombre premier $N$ de forme $4n+1$, tel qu'on eût à-la-fois $\left(\frac{c'}{N}\right)=1$, $\left(\frac{\theta}{N}\right)=1$. Ce nombre $N$ diviseroit $t^2+cu^2$, puisqu'on auroit $\left(\frac{c}{N}\right)=\left(\frac{c'\theta}{N}\right)=1$; mais l'équation $\left(\frac{\theta}{N}\right)=1$ donnant $\left(\frac{N}{\theta}\right)=1$, il s'ensuivroit que $\theta$ n'est point diviseur de $t^2+Nu^2$; donc à plus forte raison $c'\theta$ ou $c$ n'est point diviseur de cette formule. Donc il faudra encore que le diviseur quadratique de la formule $t^2+cu^2$ dans lequel $N$ est compris, soit un diviseur non réciproque.

*Remarque.* La démonstration de cette seconde partie ne pourroit plus avoir lieu, si $c$ étoit lui-même un nombre premier. Car alors il faudroit faire $\theta=c$, et $c'=1$, on auroit donc $\left(\frac{c'}{N}\right)=1$, et

---

$\left(\frac{\alpha}{N}\right)=1$, $\left(\frac{\beta}{N}\right)=1$, $\left(\frac{\gamma}{N}\right)=-1$, et ces conditions, jointes à la dernière, $\left(\frac{\theta}{N}\right)=-1$, donneront réciproquement $\left(\frac{N}{\alpha}\right)=1$, $\left(\frac{N}{\beta}\right)=1$, $\left(\frac{N}{\gamma}\right)=-1$; $\left(\frac{N}{\theta}\right)=-1$. Il est facile maintenant de résoudre chacune de ces équations (193), et en combinant ensemble les quatre résultats, on aura plusieurs expressions générales du nombre $N$, lesquelles contiendront une infinité de nombres premiers.

ainsi on ne pourroit plus satisfaire aux deux conditions $\left(\frac{c'}{N}\right) = -1$, $\left(\frac{\theta}{N}\right) = -1$, résultat qui s'accorde avec le théorême XIII.

(308) THÉORÊME XV. *Tout diviseur quadratique de première espèce est un diviseur réciproque.*

Car soit $\Delta$ un diviseur quadratique de première espèce, il y aura toujours une forme trinaire de $\Delta$ telle que les trois termes composant la valeur correspondante de $c$ ne seront pas divisibles par un même quarré. Cela posé, il a été démontré, n°. 285, que si $N$ est un nombre quelconque compris dans le diviseur $\Delta$, réciproquement $c$ sera diviseur de $t^2+Nu^2$. Donc le diviseur $\Delta$ est un diviseur réciproque.

(309) On trouve dans les Tables quelques exemples de diviseurs quadratiques dont tous les coefficiens sont divisibles par un même nombre impair. Ces diviseurs, qu'on auroit pu omettre sans inconvénient, ne sont jamais de la première espèce. En effet, soit $\Delta = py^2+2qyz+rz^2$ un de ces diviseurs, et $\theta$ un nombre premier qui divise tous ses coefficiens ; de sorte que $pr-q^2$ ou $c$ soit divisible par $\theta^2$ ; soit en même temps, $f^2\mu^2\nu^2 + g^2\nu^2\lambda^2 + h^2\lambda^2\mu^2$ la valeur de $c$ correspondante à l'une des formes trinaires de ce diviseur supposé de première espèce. On a prouvé, n°. 274, que $f^2\mu^2+g^2\lambda^2$ doit être compris dans le diviseur $\Delta$, et comme tout nombre contenu dans la fonction $\Delta$ est divisible par $\theta$, il faudra que $f^2\mu^2+g^2\lambda^2$ soit divisible par $\theta^2$. Mais le nombre total $\nu^2(f^2\mu^2+g^2\lambda^2)+h^2\lambda^2\mu^2$ est divisible par $\theta^2$ ; donc la partie $h^2\lambda^2\mu^2$ sera divisible aussi par $\theta^2$. On prouvera de même que $f^2\mu^2\nu^2$ et $g^2\nu^2\lambda^2$ sont divisibles chacun par $\theta^2$ ; donc les trois termes composant la valeur de $c$ ont un commun facteur $\theta^2$. Donc le diviseur $\Delta$ ne sauroit appartenir à la 1ère espèce.

(310) LEMME. *Si on a à-la fois* $p < \sqrt{\tfrac{4}{3}c}$, *et* $q < \tfrac{1}{2}p$, *le diviseur quadratique* $py^2+2qyz+rz^2$ *ne pourra se réduire à une expression plus simple.*

Car la réduction ne seroit possible qu'autant qu'on auroit $r < 2q$ ; or en vertu des suppositions faites, on a au contraire $r > 2q$. En effet, l'équation $pr-q^2=c$ donne $(r-2q)p = c+q^2-2pq$

$= c - \frac{1}{4}p^2 + \frac{1}{4}(p-2q)(3p-2q)$, quantité positive dans ses deux parties, puisqu'on a $c > \frac{1}{4}p^2$, et $p > 2q$. Donc $r$ est $> 2q$; donc le diviseur quadratique proposé est réduit à sa plus simple expression.

*Corollaire.* Si on a plusieurs diviseurs quadratiques $py^2 + 2qyz + rz^2$, $py^2 + 2q'yz + r'z^2$, &c. dans lesquels $p$ soit le même, et où l'on ait $p < \sqrt{\frac{4}{3}c}$, $q < \frac{1}{2}p$, $q' < \frac{1}{2}p$, &c., tous ces diviseurs seront essentiellement différens les uns des autres, et ne pourront se réduire à un moindre nombre.

(311) Lemme. *Si l'on désigne par* i *le nombre de facteurs premiers, impairs et inégaux qui divisent* c, *tout diviseur quadratique de première espèce de la formule* $t^2 + cu^2$, *ne pourra avoir plus de* $2^{i-1}$ *formes trinaires, telles que les trois termes de la valeur correspondante de* c *ne soient pas divisibles par un même quarré.*

Car soit $P$ un nombre premier plus grand que $\frac{1}{4}c^2$, contenu dans ce diviseur, et soit $K$ le nombre de forme trinaire dont ce diviseur est susceptible; le nombre $P$ aura donc, comme diviseur de la formule $t^2 + cu^2$, $K$ formes trinaires, lesquelles seront différentes les unes des autres (n°. 288), puisque $P$ supposé plus grand que $\frac{1}{4}c^2$, est à plus forte raison $> \frac{3}{4}c$. Or chacune de ces valeurs trinaires de $P$ fournit un diviseur trinaire de la formule $t^2 + Pu^2$, lequel comprendra nécessairement le nombre $c$ (n°s. 270 et 285); et ces diviseurs seront différens entr'eux, puisque les valeurs trinaires de $P$ sont différentes, et que le même diviseur quadratique de $t^2 + Pu^2$ ne peut répondre qu'à une seule forme trinaire de $P$, $P$ étant premier. Donc la formule $t^2 + Pu^2$ aura $K$ diviseurs quadratiques différens, tous renfermant le nombre $c$, et tous par conséquent de la forme $cy^2 + 2byz + az^2$, dans laquelle $c$ est coefficient du premier terme. Mais puisque $c$ est $< \sqrt{\frac{4}{3}P}$, et que dans chacun des $K$ diviseurs $cy^2 + 2byz + az^2$, on est maître de supposer $2b < c$, il s'ensuit (n°. 310) que ces $K$ diviseurs sont essentiellement différens les uns des autres. D'un autre côté, il a été démontré (n°. 233) que le nombre des diviseurs quadratiques de la formule $t^2 + Pu^2$ dans lesquels $c$ est contenu, ne peut surpasser $2^{i-1}$. Donc $K$, qui est le nombre des formes trinaires du diviseur de première espèce

$py^2 + 2qyz + rz^2$, ne pourra jamais surpasser $2^{i-1}$, si toutefois on exclut les formes trinaires pour lesquelles la valeur correspondante de $c$ auroit ces trois termes divisibles par un même quarré. En effet, sans cette exclusion, on a déjà observé que le nombre des formes trinaires dont il s'agit peut être plus grand que $2^{i-1}$, puisqu'en général il est égal au nombre de manières qu'il peut y avoir de former $c$ du produit de deux facteurs.

(312) THÉORÈME XVI. *Tout diviseur réciproque de la formule* $t^2 + Nu^2$ *est un diviseur de première espèce, et ce diviseur aura autant de formes trinaires qu'il y a d'unités dans* $2^{i-1}$, $i$ *étant le nombre des facteurs premiers impairs et inégaux qui divisent* N.

Il est facile de s'assurer que ce théorème a lieu dans les Tables VIII, IX, X et XI, au moins jusqu'à la limite où elles sont calculées. En effet, on observe d'abord que les diviseurs réciproques ne se trouvent dans aucun exemple, ni parmi les diviseurs de la seconde espèce, appelée *non décomposable*, ni parmi ceux de la troisiéme; ils appartiennent donc exclusivement à la première espèce, ce qui d'ailleurs s'accorde avec le théorême XV, où l'on a démontré que tout diviseur de première espèce est un diviseur réciproque. Si l'on parcourt ensuite les différentes formules $t^2 + cu^2$ renfermées dans les Tables, et qu'on fixe particulièrement son attention sur les diviseurs quadratiques de première espèce, on verra, comme nous l'avons déjà remarqué, que chacun de ces diviseurs se décompose en trois quarrés, d'une seule manière, si $c$ ou $\frac{1}{2}c$ est un nombre premier, et en général de $2^{i-1}$ manières s'il y a $i$ nombres premiers inégaux qui divisent $c$ ou $\frac{1}{2}c$. On trouve à la vérité une sorte d'exception lorsque $c$ est divisible par un quarré; car alors le nombre des formes trinaires de chaque diviseur de première espèce est égal au nombre de manières qu'il peut y avoir de former $c$ ou $\frac{1}{2}c$ du produit de deux facteurs quelconques; nombre plus grand que $2^{i-1}$, qui exprime (n°. XIII) combien il y a de manières de former $c$ ou $\frac{1}{2}c$ du produit de deux facteurs premiers entr'eux. Mais cette exception n'est qu'apparente, car nous avons déjà remarqué (n°. 301) que si on omet, comme n'appartenant pas à la première espèce, toutes les formes trinaires dans lesquelles

la valeur correspondante de $c$ a ses trois termes divisibles par un même facteur, le nombre des formes restantes sera toujours $2^{i-1}$, comme dans le cas où le nombre $c$ n'a aucun facteur quarré.

Par exemple, le diviseur $9y^2+6yz+14z^2$, relatif à la formule $t^2+117u^2$, est décomposable en trois formes trinaires qu'on voit dans la Table VIII; mais l'une de ces formes $(3y+z)^2+9z^2+4z^2$, répondant à la valeur trinaire $c=81+36+0$, dont les trois termes sont divisibles par un même quarré 9, on doit regarder cette forme comme étrangère à la première espèce, et en l'omettant, il ne restera que deux formes trinaires pour le diviseur dont il s'agit; nombre qui s'accorde avec la formule $2^{i-1}$, puisque 117 étant divisible par deux nombres premiers inégaux 3, 13, on a $i=2$ et $2^{i-1}=2$.

De même la formule $t^2+81u^2$ offre trois formes trinaires pour chacun de ses diviseurs de première espèce; mais de ces trois formes deux doivent être écartées, comme ne donnant pas pour $c$ une valeur exempte de diviseurs communs; il ne reste donc qu'une forme trinaire propre à la première espèce, ce qui s'accorde encore avec la formule $2^{i-1}$, où l'on a $i=1$, puisque 3 est le seul nombre premier qui divise 81.

La proposition étant ainsi vérifiée dans les Tables VIII, IX, X et XI, ou dans celle qui les comprendroit toutes, jusqu'à leur limite actuelle, ou telle autre, à laquelle on pourra parvenir par un calcul ultérieur, il s'agit de prouver en général que la formule $t^2+Nu^2$, placée immédiatement après la limite des Tables, jouira des mêmes propriétés qui ont été observées dans les précédentes, conformément à l'énoncé du théorème. Pour cela, il paroît nécessaire de diviser la proposition générale en différens cas, suivant les différentes hypothèses qu'on peut former sur la nature du diviseur proposé $cy^2+2byz+az^2$.

I$^{\text{er}}$ CAS. *Diviseur proposé* $cy^2+az^2$. (1).

(313) Dans ce premier cas, on a $ac=N$, et ainsi $c$ est divi-

(1) Dans la Table VIII, tous les diviseurs quadratiques qu'on auroit pu exprimer par $cy^2+az^2$, le sont par $cy^2+2cyz+(a+c)z^2$, ce qui est une forme équivalente.

seur de $N$; soit $k$ le nombre de facteurs premiers impairs et inégaux qui divisent $c$, on a déjà appelé $i$ le nombre de semblables facteurs qui divisent $N$, ainsi on aura $i-k$ pour le nombre de facteurs premiers impairs et inégaux qui divisent $N$ sans diviser $c$. Cela posé, puisque le diviseur proposé $cy^2+az^2$ est un diviseur réciproque, il faudra que le nombre $N$ soit diviseur de la formule $t^2+cu^2$; donc le nombre $N$ sera compris de $2^{i-k-1}$ manières dans les diviseurs quadratiques de cette formule. Mais chacun de ces diviseurs, suivant la loi générale déjà constatée pour toutes les formules qui précèdent $t^2+Nu^2$, doit avoir, puisqu'il est réciproque, $2^{k-1}$ formes trinaires. Donc le nombre $N$ aura, comme diviseur de la formule $t^2+cu^2$, $2^{k-1}\times 2^{i-k-1}$ ou $2^{i-2}$ formes trinaires. Ces valeurs trinaires qui sont toutes différentes les unes des autres (1), doivent, suivant le théor. VIII, correspondre aux diverses formes trinaires des diviseurs quadratiques de la formule $t^2+Nu^2$, dans lesquels $c$ est contenu. Or, suivant le n°. 232, $cy^2+az^2$ est le seul diviseur qui puisse contenir $c$; donc ce diviseur réunira à lui seul $2^{i-2}$ formes trinaires, dont chacune répondra à une des $2^{i-2}$ valeurs trinaires de $N$. Mais par la nature du diviseur $cy^2+az^2$, on sait (n°. 279) que la même valeur trinaire de $N$ correspond à deux formes trinaires du diviseur, excepté le cas de $c=1$ et celui de $c=2$; donc le diviseur $cy^2+az^2$, aura nécessairement $2^{i-2}\times 2$ ou $2^{i-1}$ formes trinaires, conformément à l'énoncé du théorême.

*Remarque.* L'exception qui semble avoir lieu lorsque $c=1$ ou $c=2$, vient de ce que dans ces deux cas particuliers, le nombre désigné par $2^{k-1}$ se réduit à $2^{-1}$ ou $\frac{1}{2}$; fraction à la place de laquelle on doit prendre l'unité, ainsi que nous en avons déjà prévenu (n°. 191). Au reste, bien loin que ces cas fassent exception à la règle générale, ils en sont au contraire une confirmation très-satisfaisante. Car 1°. si l'on a $c=1$, le diviseur $y^2+az^2$ ou $y^2+Nz^2$, étant supposé un diviseur réciproque de la formule $t^2+Nu^2$, il faudra que $N$ soit diviseur de $t^2+1$; donc tous les facteurs premiers

(1) Il ne peut y avoir d'exception (n°. 292) que dans le cas où on auroit $c^2=\varphi^2+N\psi^2=\varphi^2+ac\psi^2$, mais alors on auroit $c>a$, ce qui est contre la supposition.

impairs

impairs de $N$ seront de la forme $p^2+q^2$ ; donc le nombre $N$ lui-même sera autant de fois de la forme $p^2+q^2$, où $p$ et $q$ sont premiers entr'eux, qu'il y a d'unités dans $2^{i-1}$ ; mais en faisant $N=p^2+q^2$, le diviseur $y^2+Nz^2$ prend la forme trinaire $y^2+p^2z^2+q^2z^2$, laquelle répond à la valeur trinaire $N=p^2+q^2$ et appartient à la première espèce, puisque $p$ et $q$ sont premiers entr'eux ; donc le diviseur proposé $y^2+Nz^2$ aura $2^{i-1}$ formes trinaires.

2°. Si l'on a $c=2$, $N=2a$, le diviseur proposé $2y^2+az^2$ étant réciproque, il faudra que $N$ soit diviseur de $t^2+2$ ; donc tous les facteurs premiers impairs de $N$ seront de la forme $p^2+2q^2$. Donc le nombre $N$ lui-même sera $2^{i-1}$ fois de la forme $p^2+2q^2$, $p$ et $q$ étant premiers entr'eux. Or si on considère la valeur $N=f^2+2g^2=2a$, et qu'on fasse $f=2m$, on aura $a=2m^2+g^2$, et $2y^2+az^2=2y^2+2m^2z^2+g^2z^2=(y+mz)^2+(y-mz)^2+g^2z^2$ ; d'où l'on voit que chaque valeur trinaire de $N$, telle que $f^2+g^2+g^2$, donne une forme trinaire pour le diviseur $2y^2+az^2$ ; donc ce diviseur aura encore $2^{i-1}$ formes trinaires différentes, et propres à la première espèce.

### IIe Cas. *Diviseur proposé* $2by^2+2byz+az^2$.

(314) Dans ce cas, on aura $N=2ab-bb$, et $b$ sera encore diviseur de $N$. Soit toujours $k$ le nombre des facteurs premiers et inégaux qui divisent $b$, on aura $i-k$ pour le nombre des facteurs premiers, inégaux qui divisent $N$ sans diviser $b$ ; mais puisque le diviseur proposé est réciproque, il faudra que $N$ soit diviseur de $t^2+2bu^2$ ; donc le nombre $N$ sera contenu $2^{i-k-1}$ fois dans les diviseurs quadratiques de la formule $t^2+2bu^2$, et comme chacun de ces diviseurs se développe en $2^{k-1}$ formes trinaires, il s'ensuit que le nombre $N$ aura, comme diviseur de la formule $t^2+2bu^2$, $2^{k-1}\times 2^{i-k-1}$ ou $2^{i-2}$ formes trinaires (1). Ces valeurs doivent par

(1) Ces valeurs trinaires sont toutes différentes entr'elles ; car s'il y avoit exception, il faudroit qu'on eût $(2b)^2=\varphi^2+N\psi^2=\varphi^2+(2ab-bb)\psi^2$. Or comme on doit avoir $a>b$, cette équation donne d'abord $\psi=1$, ensuite $\varphi=b$, $b=1$ et $a=2$ : on tombe ainsi dans le cas de $N=3$, où le diviseur $2y^2+2yz+2z^2$ n'a qu'une forme trinaire $y^2+z^2+(y+z)^2$ conformément à la formule $2^{i-1}$.

conséquent résulter aussi des diverses formes trinaires dont est susceptible le diviseur $2by^2+2byz+az^2$, le seul qui contienne $2b$ parmi les diviseurs quadratiques de la formule $t^2+Nu^2$; d'ailleurs par la nature du diviseur $2by^2+2byz+az^2$ (n°. 279) la même valeur trinaire de $N$ répond à deux formes trinaires du diviseur. Donc ce diviseur aura en tout $2^{i-1}$ formes trinaires, conformément à la loi générale.

*Remarque I.* La démonstration qu'on vient de donner de ce second cas, ne suppose autre chose que la condition ordinaire $a>b$; elle est donc aussi applicable au cas où le diviseur proposé seroit $ay^2+2byz+az^2$, car celui-ci peut se mettre sous la forme $ay^2+(2a-2b)yz+(2a-2b)z^2$, laquelle rentre dans le cas qu'on vient d'examiner.

*Remarque II.* La démonstration précédente paroît encore présenter une sorte d'exception lorsque $b=1$, ou lorsque le diviseur proposé est $2y^2+2yz+az^2$. Mais comme alors le nombre $N$ doit être diviseur de $t^2+2$, il faudra que ce nombre soit $2^{i-1}$ fois de la forme $p^2+2q^2$; soit une de ces valeurs $N=f^2+2g^2=2a-1$, on aura $a=\frac{1}{2}(f^2+1)+g^2$, et $2y^2+2yz+az^2=(y+\frac{1}{2}(f+1)z)^2+[y-\frac{1}{2}(f-1)z]^2+g^2z^2$; donc le diviseur proposé aura encore $2^{i-2}$ formes trinaires.

III$^e$ CAS. *Le plus petit coefficient* c *du diviseur* $cy^2+2byz+az^2$ *est supposé premier ou double d'un premier.*

(315) Si le nombre $c$ ou $\frac{1}{2}c$ étoit diviseur de $N$, ce cas rentreroit dans l'un ou l'autre des deux précédens, ainsi nous pourrons supposer que $N$ n'est divisible ni par $c$ ni par $\frac{1}{2}c$. Cela posé, puisque le diviseur $cy^2+2byz+az^2$ est réciproque, il faudra que $N$ soit diviseur de $t^2+cu^2$, et par conséquent que $N$ soit contenu $2^{i-1}$ fois dans les diviseurs quadratiques de la formule $t^2+cu^2$. Mais ces diviseurs dans lesquels $N$ est contenu devant être réciproques, ils seront tous de première espèce, et auront chacun une forme trinaire, puisque la proposition générale a été vérifiée pour toutes les formules qui précèdent $t^2+Nu^2$; donc le nombre $N$, comme diviseur de $t^2+cu^2$, aura $2^{i-1}$ formes trinaires, lesquelles seront différentes entr'elles, sauf le cas où l'on auroit $c^2=\varphi^2+N\psi^2$.

Mais $c^2$ étant plus petit que $\frac{4}{3}N$, si l'exception a lieu, il faudra qu'on ait $\psi=1$ et $c^2=\varphi^2+N$. Dans ce cas particulier, $cy^2+2\varphi yz+cz^2$ seroit aussi un diviseur quadratique de la formule $t^2+Nu^2$, et ce diviseur contiendroit, comme on voit, le nombre $c$; mais le nombre $c$ premier, ou double d'un premier, ne sauroit appartenir à deux diviseurs quadratiques différens. Il faudra donc que le diviseur proposé $cy^2+2byz+az^2$ coincide avec le diviseur $cy^2+2\varphi yz+cz^2$. Or celui-ci pouvant se mettre sous la forme $cy^2+(2c-2\varphi)yz+(2c-2\varphi)z^2$, laquelle rentre dans le deuxième cas, il s'ensuit que le nombre des formes trinaires du diviseur proposé sera égal à $2^{i-1}$. Il ne reste par conséquent à examiner que le cas principal dans lequel les $2^{i-1}$ valeurs trinaires de $N$ sont différentes les unes des autres. Alors chacune de ces valeurs devant répondre à une forme trinaire du diviseur $cy^2+2byz+az^2$, il faudra que celui-ci ait encore $2^{i-1}$ formes trinaires, conformément à l'énoncé du théorême.

IV$^e$ CAS. *On suppose que le diviseur proposé contient un nombre* P *premier ou double d'un premier, et moindre que* N.

(316) La démonstration sera la même que dans le cas précédent, parce qu'on peut toujours, par une transformation, faire en sorte que le premier coefficient $c$ du diviseur proposé $cy^2+2byz+az^2$ soit égal au nombre $P$, ainsi on pourra encore supposer que $c$ est premier ou double d'un premier; mais au lieu d'avoir $c<\sqrt{\frac{4}{3}N}$, on aura seulement $c<N$; et il reste à examiner quels peuvent être les cas d'exception contenus dans l'équation $c^2=\varphi^2+N\psi^2$.

Soit d'abord $\psi$ impair, et en général $\psi=\alpha\zeta$, $\alpha$ et $\zeta$ étant deux facteurs indéterminés; soit en même temps $N=\mathcal{A}B$, $\mathcal{A}$ et $B$ étant de semblables facteurs, l'équation $c^2-\varphi^2=N\psi^2$ ne pourra se décomposer que de cette manière:

$$c+\varphi=\mathcal{A}\alpha^2$$
$$c-\varphi=B\zeta^2,$$

d'où résulte $2c=\mathcal{A}\alpha^2+B\zeta^2$; car toute autre décomposition rendroit $c$ divisible par un facteur impair de $\psi$, ce qui ne peut s'accorder avec la supposition que $c$ est premier ou double d'un premier. Maintenant puisque $N=\mathcal{A}B$, on voit que $\mathcal{A}y^2+Bz^2$ est

un diviseur quadratique de la formule $t^2+Nu^2$; ce diviseur contient $2c$, puisqu'on vient de trouver $2c=A\alpha^2+B6^2$; donc $c$ doit être contenu dans le diviseur conjugué de $Ay^2+Bz^2$ : or j'observe que les nombres $A$ et $B$ ne peuvent être qu'impairs d'après l'équation $2c=A\alpha^2+B6^2$; car si $A$, par exemple, étoit pair, il faudroit que $B$ le fût, et ainsi $AB$ ou $N$ seroit divisible par 4, ce qui ne peut jamais avoir lieu. Soit donc $A>B$ et $A+B=2C$, le diviseur $Ay^2+Bz^2$ étant le même que $(A+B)y^2+2Byz+Bz^2$, ou $2Cy^2+2Byz+Bz^2$, son conjugué sera $Cy^2+2Byz+2Bz^2$; de sorte que le nombre $c$ doit être compris dans la formule $Cy^2+2Byz+2Bz^2$. Mais le nombre $c$, qui est premier ou double d'un premier, ne peut pas être contenu dans deux diviseurs quadratiques différens; donc le diviseur proposé $cy^2+2byz+az^2$, lorsqu'il aura été réduit à l'expression la plus simple, sera identique avec $Cy^2+2Byz+2Bz^2$. Et puisque celui-ci est compris dans le deuxième cas, il s'ensuit que le diviseur proposé $cy^2+2byz+az^2$ aura $2^{i-1}$ formes trinaires, conformément à la loi générale.

En second lieu, soit $\psi$ pair, si l'on fait $\psi=2\alpha6$ et $N=AB$, l'équation $c^2-\varphi^2=N\psi^2$ ne pourra se décomposer que de l'une de ces deux manières :

$$\left.\begin{array}{l} c\pm\varphi=A\alpha^2 \\ c\mp\varphi=4B6^2 \end{array}\right\} (1) \qquad\qquad \left.\begin{array}{l} c+\varphi=2A\alpha^2 \\ c-\varphi=2B6^2 \end{array}\right\} (2)$$

La première combinaison donne $2c=A\alpha^2+4B6^2$, et il faudra, dans ce cas, que l'un des nombres $A$, $\alpha$ soit pair. Soit 1°. $A=2C$, et on aura $c=C\alpha^2+2B6^2$, d'où l'on voit que le nombre $c$ est compris dans le diviseur quadratique $Cy^2+2Bz^2$; donc le diviseur proposé doit être identique avec $Cy^2+2Bz^2$; mais celui-ci rentre dans le premier cas général (n°. 313), puisqu'on a $2BC=N$; donc le diviseur proposé aura encore, dans ce cas particulier, $2^{i-1}$ formes trinaires. Soit 2°. $\alpha=2\gamma$, on aura $c=2A\gamma^2+2B6^2$; de sorte que le nombre $\frac{1}{2}c$ est compris dans le diviseur quadratique $Ay^2+Bz^2$, donc le nombre $c$ sera compris dans son conjugué. Or si l'un des deux nombres $A$ et $B$ est pair, par exemple $A$, le diviseur conjugué de $Ay^2+Bz^2$ sera $\frac{1}{2}Ay^2+2Bz^2$, ce qui rentre dans le Cas premier; et si les deux nombres $A$ et $B$ sont

impairs, le diviseur conjugué de $Ay^2+Bz^2$ sera $\frac{1}{2}(A+B)\,y^2+2Byz+2Bz^2$, ce qui rentre dans le deuxième Cas.

Enfin la seconde combinaison donnant $2c=2A\alpha^2+2B\mathcal{C}^2$, ou $c=A\alpha^2+B\mathcal{C}^2$, le nombre $c$ est compris immédiatement dans le diviseur quadratique $Ay^2+Bz^2$, ce qui retombe dans le Cas I$^{er}$.

Donc pourvu que le diviseur proposé $cy^2+2byz+az^2$ contienne un seul nombre premier ou double d'un premier, moindre que $N$, ce diviseur aura nécessairement $2^{i-1}$ formes trinaires, propres à la première espèce.

*Remarque.* Ce quatrième Cas est tellement étendu, qu'il n'y a aucune formule des Tables qui n'y soit comprise; et les exceptions paroissant devoir se présenter le plus facilement dans les petits nombres, il est probable qu'il embrasse de même toutes les formules ultérieures.

V$^e$ Cas. *On suppose que le diviseur proposé* $cy^2+2byz+az^2$ *contient un nombre* $c<N$, *dont tous les facteurs premiers, à l'exception d'un seul, sont diviseurs de* N *et inégaux entr'eux.*

(317) Soit alors $c=\theta c'$, $N=\theta N'$, $\theta$ étant le plus grand diviseur commun entre $c$ et $N$, et $c'$ étant un nombre premier ou double de premier. Soit $k$ le nombre de facteurs premiers, impairs qui divisent $c$: on a déjà appelé $i$ le nombre de facteurs premiers et inégaux qui divisent $N$; donc $i-k+1$ sera le nombre de facteurs premiers qui divisent $N$ sans diviser $c$. Cela posé, le nombre $N$ devant être diviseur de $t^2+cu^2$, sera compris de $2^{i-k}$ manières différentes dans les diviseurs quadratiques de cette formule; de plus, comme chaque diviseur réciproque de la formule $t^2+cu^2$ doit avoir $2^{k-1}$ formes trinaires, il s'ensuit que le nombre $N$, comme diviseur de $t^2+cu^2$, aura $2^{k-1}.2^{i-k}$ ou $2^{i-1}$ valeurs trinaires. Or chacune de ces valeurs doit correspondre à une forme trinaire de l'un des diviseurs quadratiques de la formule $t^2+Nu^2$ dans lesquels $c$ est contenu; et comme dans l'hypothèse de ce cinquième Cas, le diviseur proposé $cy^2+2byz+az^2$ est le seul qui puisse contenir $c$, il s'ensuit que ce diviseur aura nécessairement $2^{i-1}$ formes trinaires.

*Remarque.* Ce Cas, qui est encore plus général que les précédens, n'est sujet à aucune exception. En effet, si on avoit $c^2 = \varphi^2 + N\psi^2$, comme on suppose que $\theta$ qui divise $c$ et $N$ n'a que des facteurs simples, il faudra que $\varphi$ soit divisible par $\theta$, et alors $N\psi^2$ doit l'être par $\theta^2$. Mais on fera voir dans une note du Cas suivant, que $N$ ne peut être divisible par le quarré $\alpha^2$, si $c$ est divisible seulement par $\alpha$; donc $N\psi^2$ ne peut être divisible par $\theta^2$, à moins que $\psi$ ne soit divisible par $\theta$. Faisant donc $\varphi = \theta\varphi'$, $\psi = \theta\psi'$, on aura $c'^2 - \varphi'^2 = N\psi'^2$. Dans cette équation $c'$ est un nombre premier ou le double d'un nombre premier; ainsi on démontrera, comme dans le Cas précédent, que $c'$ appartient soit au diviseur quadratique $Ay^2 + Bz^2$, soit à son conjugué $\frac{1}{2}(Ay^2 + Bz^2)$. Or ayant $AB = N = N'\theta$, si l'on fait $N' = PQ$, $\theta = \gamma\delta$, on pourra supposer $A = P\gamma$, $B = Q\delta$, et on aura $c' = P\gamma y^2 + Q\delta z^2$, ou $c' = \frac{1}{2}(P\gamma y^2 + Q\delta z^2)$; donc $\gamma\delta c' = P\delta\gamma^2 y^2 + Q\gamma\delta^2 z^2$, ou $\gamma\delta c' = \frac{1}{2}(P\delta\gamma^2 y^2 + Q\gamma\delta^2 z^2)$. De-là on voit que $c$ est compris soit dans le diviseur quadratique $P\delta y^2 + Q\gamma z^2$, soit dans son conjugué représenté par $\frac{1}{2}(P\delta y^2 + Q\gamma z^2)$. Mais comme $c$ ne peut être compris que dans un seul diviseur quadratique, il s'ensuit que si on avoit $c^2 = \varphi^2 + N\psi^2$, le diviseur proposé rentreroit dans les Cas I ou II, et ainsi il auroit toujours $2^{i-1}$ formes quadratiques, conformément à l'énoncé du théorême.

VI[e] CAS. *On suppose que le diviseur proposé* $cy^2 + 2byz + az^2$ *contient un nombre* c *moindre que* N, *lequel n'a aucun facteur quarré commun avec* N.

(318) Pour ne pas revenir inutilement sur les Cas déjà examinés, nous supposerons que $c$ ou $\frac{1}{2}c$ n'est ni un nombre premier, ni un diviseur de $N$, ni le produit des deux; il y aura donc plusieurs diviseurs quadratiques de la formule $t^2 + Nu^2$ qui contiendront $c$. Soit $k$ le nombre de facteurs premiers impairs et inégaux qui divisent $c$, soit $e$ le nombre de ces facteurs qui sont communs entre $N$ et $c$, et par conséquent $k - e$ le nombre des facteurs premiers qui divisent $c$ sans diviser $N$ (1), la formule $2^{k-e-1}$ représentera

(1) Lorsque $c$ est compris dans un diviseur quadratique de la formule $t^2 + Nu^2$,

le nombre des diviseurs $cy^2+2byz+az^2$ qui ont $c$ pour coefficient du premier terme (n°. 243). Or on va prouver que tous ces diviseurs sont de première espèce, et que chacun d'eux a nécessairement $2^{i-1}$ formes trinaires.

Puisque le nombre $N$ est divisible par $i$ nombres premiers différens dont $e$ sont communs avec $c$, il y a $i-e$ facteurs premiers impairs qui divisent $N$ sans diviser $c$. Donc, puisque $N$ est diviseur de la formule $t^2+cu^2$, le nombre $N$ sera contenu de $2^{i-e-1}$ manières dans les diviseurs quadratiques de la formule $t^2+cu^2$. Ceux-ci ont chacun $2^{k-1}$ formes trinaires, en vertu de la proposition générale qui est constatée pour toutes les formules $t^2+cu^2$ où $c$ est moindre que $N$, et qui sont de nature à être comprises dans les Tables. Donc le nombre $N$, considéré comme diviseur de la formule $t^2+cu^2$, aura $2^{k-1}.2^{i-e-1}$ formes trinaires, lesquelles seront différentes les unes des autres, sauf quelques cas particuliers qu'on peut éviter en changeant la valeur de $c$, comme il sera dit ci-après. Mais de chaque valeur trinaire de $N$ on peut déduire une forme trinaire pour l'un des diviseurs quadratiques de la formule $t^2+Nu^2$ dans lesquels $c$ est contenu. Donc le nombre des formes trinaires de tous les diviseurs $cy^2+2byz+az^2$ sera également $2^{k-1}.2^{i-e-1}$.

Maintenant on a déjà vu qu'il existe $2^{k-e-1}$ diviseurs quadratiques $cy^2+2byz+az^2$ dont $c$ est coefficient du premier terme; et puisque les formes trinaires réunies de tous ces diviseurs composent le nombre total $2^{k-1}.2^{i-e-1}$, il s'ensuit que si ces diviseurs ont chacun un égal nombre de formes trinaires, ce nombre sera $\frac{2^{k-1}.2^{i-e-1}}{2^{k-e-1}}$ ou $2^{i-1}$. Donc s'ils n'avoient pas tous le même nombre

---

et réciproquement $N$ dans un diviseur de $t^2+cu^2$, si les deux nombres $c$ et $N$ sont divisibles par un même nombre premier $\theta$, il faudra qu'aucun d'eux ne soit divisible par $\theta^2$ ou qu'ils le soient tous deux par $\theta^2$. Car $N'\theta^2$, par exemple, ne peut être diviseur de $t^2+c'\theta$, à moins que $c'$ ne soit aussi divisible par $\theta$. Donc puisqu'on exclut dans ce V$^e$ Cas les facteurs quarrés communs entre $c$ et $N$, il faudra que le plus grand commun diviseur entre $c$ et $N$ n'ait que des facteurs premiers inégaux. C'est par cette raison que $k-e$ représente le nombre de facteurs premiers qui divisent $c$ sans diviser $N$.

de formes trinaires, il faudroit qu'un ou plusieurs d'entr'eux eussent plus de $2^{i-1}$ de ces formes. Or on a prouvé (n°. 311) qu'aucun diviseur quadratique $cy^2+2byz+az^2$ ne peut avoir plus de $2^{i-1}$ formes trinaires, propres à la première espèce ; donc enfin le diviseur proposé $cy^2+2byz+az^2$ et tous ceux qui contiennent le même nombre $c$, auront chacun $2^{i-1}$ formes trinaires. On voit de plus que tous ces diviseurs doivent être différens les uns des autres (1).

---

(1) Pour rendre ces raisonnemens plus sensibles par un exemple, soit $21y^2+26yz+174z^2$ un diviseur proposé de la formule $t^2+3485u^2$, lequel est réciproque, parce qu'il est facile de s'assurer que 3485 ou 5 . 17 . 41 est diviseur de $t^2+21u^2$. On aura, dans ce cas, $N=3485$, $c=21$, et parce que $N$ est composé du produit de trois facteurs dont aucun ne divise $c$, on aura $i=3$, $e=0$; de même puisque $c$ est le produit de deux facteurs 3 . 7, on aura $k=2$. Or on voit d'abord que $N$ doit être contenu de $2^{3-1}$ ou 4 manières dans les diviseurs quadratiques de la formule $t^2+21u^2$, ou seulement dans le diviseur $5y^2+6yz+6z^2$, parce que celui-ci est seul de son espèce ; d'ailleurs ce dernier diviseur se décompose de $2^{k-1}$ ou 2 manières en trois quarrés ; donc le nombre $N$, comme diviseur de la formule $t^2+cu^2$, aura 4 . 2 ou 8 formes trinaires différentes, lesquelles sont en effet,

$$51^2+28^2+10^2,\quad 53^2+24^2+10^2,\quad 51^2+20^2+22^2,\quad 34^2+27^2+40^2,$$
$$18^2+56^2+5^2,\quad 34^2+48^2+5^2,\quad 42^2+40^2+11^2,\quad 13^2+54^2+20^2.$$

Il faudra donc que les diverses formes trinaires de tous les diviseurs de la formule $t^2+3485u^2$, dans lesquels $c$ est contenu, répondent à ces 8 formes trinaires de $N$. Les diviseurs dont il s'agit, au nombre de $2^{k-e-1}=2$, sont le diviseur proposé $21y^2+26yz+174z^2$, et un autre $21y^2+2yz+166z^2$; or chacun d'eux ne peut avoir plus de $2^{i-1}$ ou 4 formes trinaires; donc les 8 formes trinaires dont il s'agit, réparties entre eux deux, en donneront nécessairement 4 à chacun. En effet, on trouve ces quatre formes et les valeurs correspondantes de $N$, comme il suit :

$$\left.\begin{array}{l} 40^2+42^2+11^2 \\ 56^2+18^2+5^2 \\ 40^2+34^2+27^2 \\ 48^2+34^2+5^2 \end{array}\right\} 21y^2+2yz+166z^2=\left\{\begin{array}{l} (4y+6z)^2+(2y-7z)^2+(y-9z)^2 \\ (4y-6z)^2+(2y+11z)^2+(y+3z)^2 \\ (4y-2z)^2+(2y+9z)^2+(y-9z)^2 \\ (4y-6z)^2+(2y+9z)^2+(y+7z)^2 \end{array}\right.$$

$$\left.\begin{array}{l} 51^2+28^2+10^2 \\ 53^2+24^2+10^2 \\ 51^2+20^2+22^2 \\ 54^2+20^2+13^2 \end{array}\right\} 21y^2+26yz+174z^2=\left\{\begin{array}{l} (4y+z)^2+(2y-2z)^2+(y+13z)^2 \\ (4y-z)^2+(2y+2z)^2+(y+13z)^2 \\ (4y+7z)^2+(2y-2z)^2+(y-11z)^2 \\ (4y+7z)^2+(2y-10z)^2+(y+5z)^2 \end{array}\right.$$

La démonstration eût été plus simple pour le diviseur $21y^2+2yz+166z^2$ en par-

(319) Ce VI[e] Cas est d'une très-grande généralité, puisqu'il suppose seulement que le nombre $c$ contenu dans le diviseur quadratique proposé est moindre que $N$, et n'a aucun facteur quarré commun avec $N$. Mais pour mieux juger de cette généralité, il est nécessaire de déterminer d'une manière précise combien il peut y avoir de semblables nombres contenus dans le diviseur quadratique proposé $cy^2+2byz+az^2=\Delta$.

Ayant donné à $z$ une valeur déterminée $z=k$, si l'on veut avoir toutes les valeurs de $y$ qui rendent $\Delta$ moindre que $N$, il faudra résoudre l'équation $N=cy^2+2byk+ak^2$, laquelle donne les limites de $y$, savoir :

$$y=\frac{-bk-\sqrt{(cN-k^2N)}}{c}\ ,\quad y=\frac{-bk+\sqrt{(cN-k^2N)}}{c}.$$

La différence de ces deux limites $\frac{2\sqrt{N}}{c}\cdot\sqrt{(c-k^2)}$ exprime donc le nombre de valeurs qu'on peut donner à $y$, tandis qu'on fait $z=k$; elle apprend en même temps que la plus grande valeur qu'on puisse donner à $z$ est $\sqrt{c}$ ou l'entier compris dans $\sqrt{c}$. De-là on voit que le nombre de tous les diviseurs moindres que $N$ compris dans le diviseur quadratique $\Delta$ sera donné par la formule

$$X=\frac{2\sqrt{N}}{c}[\sqrt{c}+\sqrt{(c-1)}+\sqrt{(c-4)}+\sqrt{(c-9)}+\text{\&c.}],$$

cette suite devant être continuée tant que les termes en sont réels.

J'observe maintenant que si on décrit un cercle qui ait pour équation $y^2=R^2-x^2$, et que $R$ soit un nombre un peu grand, l'aire du quart de ce cercle sera à très-peu près égale à la somme de la suite $R+\sqrt{(R^2-1)}+\sqrt{(R^2-4)}+\sqrt{(R^2-9)}+$ &c. continuée tant que les termes sont réels. Donc comme on sait que l'aire du quart de cercle $=\frac{1}{4}\pi R^2$, $\pi$ étant le rapport de la circonférence au diamètre, il faut que la somme de cette dernière suite soit $\frac{\pi}{4}R^2$, valeur d'autant plus approchée, que $R$ sera plus grand.

Cela posé, si on met simplement $c$ à la place de $R^2$, on aura

---

ticulier, si l'on eût considéré $N$ comme diviseur de $t^2+166u^2$, car alors on seroit retombé dans le IV[e] Cas.

$X = \frac{2\sqrt{N}}{c} \cdot \frac{\pi}{4} c = \frac{\pi}{2}\sqrt{N}$; résultat remarquable, en ce qu'il ne dépend plus des coefficiens $a$, $b$, $c$, et qu'il est le même pour tous les diviseurs quadratiques d'une même formule $t^2+Nu^2$ (1).

La valeur de $X$ qu'on vient de trouver, suppose qu'on a pris indifféremment pour $y$ et $z$ toutes les valeurs qui peuvent rendre $cy^2+2byz+az^2$ moindre que $N$, mais il faut se rappeler que les seuls résultats admissibles sont ceux où $y$ et $z$ n'ont pas de commun diviseur. Or les cas où $y$ et $z$ sont tous deux pairs forment le quart de tous les cas possibles ; ceux où $y$ et $z$ sont à-la-fois divisibles par 3, forment la neuvième partie de la totalité, et ainsi de suite. Donc en général le nombre trouvé $X$ doit se réduire à $X(1-\frac{1}{4})(1-\frac{1}{9})(1-\frac{1}{25})(1-\frac{1}{49})$ &c., les dénominateurs de ces fractions étant les quarrés des nombres premiers successifs. Mais on sait que le produit $(1-\frac{1}{4})(1-\frac{1}{9})(1-\frac{1}{25})(1-\frac{1}{49})$ &c. continué à l'infini $= \frac{6}{\pi\pi}$ (Voyez l'*Introduct. in Anal.* d'Euler, n°. 277). Donc si on appelle $Y$ le nombre des diviseurs particuliers, moindres que $N$, compris dans le diviseur quadratique proposé $cy^2+2byz+az^2$, on aura $Y = \frac{\pi}{2}\sqrt{N} \cdot \frac{6}{\pi\pi} = \frac{3}{\pi}\sqrt{N}$. Formule très-simple, et qui dans les applications donne des résultats fort proches de la vérité.

(320) Soit maintenant $\alpha$ un nombre premier dont le quarré est diviseur de $N$, en sorte qu'on ait $N = \alpha^2 N'$. Si l'on suppose $c$ divisible par $\alpha$, il faudra que $b$ soit aussi divisible par $\alpha$, puisqu'on a $ac-b^2=N$; mais les deux termes $b^2$ et $N$ étant alors divisibles par $\alpha^2$, on voit que $ac$ doit être aussi divisible par $\alpha^2$; donc comme on ne peut supposer $a$ divisible par $\alpha$, puisqu'alors

(1) Ce résultat devroit être réduit à moitié, si la formule proposée étoit de l'une des formes $cy^2+az^2$, $cy^2+2byz+bz^2$, $cy^2+2byz+cz^2$, parce qu'alors le même nombre résulte de deux suppositions différentes dans les valeurs de $y$ et de $z$. On retrouve donc ici les mêmes exceptions auxquelles ces formules donnent lieu dans d'autres occasions.

les trois termes du diviseur quadratique proposé seroient divisibles par $\alpha$, il faut que $c$ soit divisible par $\alpha^2$, ce qui s'accorde d'ailleurs avec la note du n°. 318. Dans ce cas, si on donne à $y$ une valeur déterminée $h$, et qu'on fasse successivement $z=0, 1, 2, 3$, &c. aussi bien que $z=-1, -2, -3, -4$, &c., la suite provenant du terme général $ch^2+2bhz+az^2$ sera telle, que sur $\alpha$ termes consécutifs, il y en aura un divisible par $\alpha^2$. La même chose aura lieu, quand même $c$ ne seroit pas divisible par $\alpha$; car on peut trouver aisément une valeur de $z$ telle que $ch^2+2bhz+az^2$ soit divisible par $\alpha^2$; pour cela, supposant $ch^2+2bhz+az^2=\alpha^2P$, et multipliant cette équation par $c$, on aura $(ch+bz)^2+Nz^2=c\alpha^2P$; donc il suffit de déterminer $z$ de manière que $ch+bz$ soit divisible par $\alpha$. Cette valeur de $z$ étant trouvée et désignée par $k$, si l'on fait en général $z=k+\alpha z'$, toutes les valeurs de $z$ contenues dans cette formule rendront la quantité $ch^2+2bhz+az^2$ divisible par $\alpha^2$; donc sur $\alpha$ termes consécutifs de la série dont le terme général est $ch^2+2bhz+az^2$, il y en aura toujours un qui sera divisible par $\alpha^2$.

De-là on voit que si on eût conservé tous les termes dont $X$ est le nombre, il auroit fallu multiplier le nombre de ces termes par $1-\frac{1}{\alpha}$, afin d'en retrancher les termes divisibles par $\alpha^2$; mais pour supprimer les termes où $y$ et $z$ sont divisibles par $\alpha$, on a déjà employé le facteur $1-\frac{1}{\alpha^2}$, par lequel $X$ a été multiplié; donc il reste encore à diviser le résultat par $1+\frac{1}{\alpha}$, ou à le multiplier par $\frac{\alpha}{\alpha+1}$, afin de faire disparoître dans $Y$ tous les termes divisibles par $\alpha^2$.

Soient donc $\alpha$, $\mathcal{C}$, $\gamma$, &c. les différens nombres premiers dont les quarrés peuvent diviser $N$; si on appelle $z$ le nombre des diviseurs qui étant contenus dans la formule proposée $cy^2+2byz+az^2$, sont moindres que $N$, et n'ont aucun facteur quarré commun avec $N$, on aura en général $Z=\frac{3\sqrt{N}}{\pi}\cdot\frac{\alpha}{\alpha+1}\cdot\frac{\mathcal{C}}{\mathcal{C}+1}\cdot\frac{\gamma}{\gamma+1}\cdot$ &c.,

ou bien faisant $N = M.\alpha^2 \mathcal{C}^2 \gamma^2$, &c., on aura $Z = \frac{3\sqrt{M}}{\pi} \cdot \frac{\alpha^2}{\alpha+1} \cdot \frac{\mathcal{C}^2}{\mathcal{C}+1} \cdot \frac{\gamma^2}{\gamma+1} \cdot$ &c. D'où l'on voit que $Z$ est un nombre qui augmente en même temps que $N$, et qui aura toujours un rapport notable avec $\sqrt{N}$.

Par exemple, si on propose le diviseur quadratique $189y^2 + 30yz + 50z^2$ appartenant à la formule $t^2 + 9225u^2$, et qu'on veuille savoir combien dans ce diviseur il y a de nombres plus petits que 9225, et qui n'ont aucun facteur quarré commun avec 9225, on fera $N = 9225 = 3^2.5^2.41$, ce qui donnera $\alpha = 3$, $\mathcal{C} = 5$, $M = 41$; d'où l'on conclura le nombre cherché $Z = \frac{3\sqrt{41}}{\pi} \cdot \frac{9}{4} \cdot \frac{25}{6} = 57\frac{1}{3}$; et ce résultat est très-près de la vérité ; car on trouve que le diviseur proposé contient les 59 nombres suivans qui ont les conditions mentionnées :

209, 269, 329, 449, 746; 866, 869, 1109, 1289, 1589; 1661, 1706, 1721, 1841, 2081; 2141, 2306, 2429, 2501, 2786; (2849), 2861, 2954, 3149, 3194; 3401, 3521, (3626), 3629, 3674; (4181), 4634, 4781, 4874, 4889; 5489, (5621), 5801, 5909, 6146; 6314, 6569, 6674, 6761, 7034; (7154), 7466, 7601, 7754, 7994; (8249), 8426, 8741, (8954), 8981; 9029, 9041, 9101, 9221.

(321) On voit maintenant que le VI[e] Cas renferme la démonstration générale de la proposition, puisqu'il y aura toujours un nombre assez considérable de valeurs de $c$ qui pourront servir de base à la démonstration. Or il suffit qu'il y ait parmi ces valeurs un diviseur de $N$ ou $2N$ (Cas I et II), ou un nombre premier ou double d'un premier (Cas IV), ou le produit d'un tel nombre par un diviseur de $N$ (Cas V), ou enfin un nombre quelconque qui ne satisfasse pas à l'équation $c^2 = \varphi^2 + N\psi^2$. Il pourroit cependant arriver que tous les nombres $c$ compris dans le diviseur proposé, satisfissent à l'équation $c^2 = \varphi^2 + N\psi^2$, mais alors (n°. 316) ce diviseur seroit de la forme $cy^2 + az^2$, ou $\frac{1}{2}(cy^2 + az^2)$, et ainsi il retomberoit dans les Cas I ou II, qui sont les plus simples de tous.

L'exemple que nous avons apporté du diviseur quadratique $189y^2+30yz+50z^2$ est un des plus désavantageux, parce que les nombres 189 et 50, ont l'un et l'autre un facteur quarré commun avec $N=9225$; néanmoins nous avons trouvé 59 nombres, entre lesquels on peut choisir pour avoir une valeur convenable de $c$. Or la suite de ces nombres présente immédiatement des nombres premiers ou doubles de premiers, tels que 269, 449, 746, 866, &c. D'où on conclura aussi-tôt (par le Cas IV) que le diviseur proposé $189y^2+30yz+50z^2$ se décompose de $2^{3-1}$ ou 4 manières en trois quarrés. Et la même conclusion se déduiroit aussi (par le Cas VI) de tous les autres nombres 209, 329, &c., excepté seulement ceux qui satisferoient à l'équation $c^2=\phi^2+N\psi^2$. Or ceux-ci, qui sont distingués par des parenthèses, ne sont qu'au nombre de sept; de sorte qu'il reste 52 nombres différens, également propres à être pris pour $c$, et dont un seul suffit pour établir la démonstration.

(322) Dans l'exemple cité, la formule $t^2+Nu^2$ a cinq diviseurs quadratiques réciproques, savoir :

$$9y^2+1025z^2$$
$$225y^2+41z^2$$
$$125y^2+60yz+81z^2$$
$$125y^2+10yz+74z^2$$
$$189y^2+30yz+50z^2.$$

Les deux premiers étant de la forme $cy^2+az^2$, sont relatifs au Cas I; le troisième contenant le nombre $125-60+81=146$, double d'un premier, est compris dans le Cas IV; le quatrième est compris dans le même Cas, puisque 74 est un de ses coefficiens; enfin le cinquième est celui que nous avons examiné spécialement, et où d'ailleurs on trouve immédiatement le nombre premier $189+30+50=269$. Ainsi un examen très-superficiel des diviseurs proposés, dans cet exemple comme dans tous les autres qui pourront se présenter, suffit pour décider que ces diviseurs sont de première espèce, et que le nombre de leurs formes trinaires est conforme à la loi générale. On voit de plus, par le nombre et la nature de ces diviseurs, combien le nombre $N$ doit avoir de formes trinaires. Les deux premiers supposent chacun deux formes trinaires dis-

tinctes, les trois autres en supposent chacun quatre; ainsi le nombre 9225 doit avoir en tout $2\times2+3\times4$ ou 16 formes trinaires, résultat facile à vérifier. Ces seize formes d'ailleurs doivent être propres à la première espèce, c'est-à-dire, telles que leurs trois termes ne soient pas divisibles par un même quarré.

Les cinq diviseurs quadratiques précédens, et en général le système des diviseurs de première espèce pour une formule quelconque $t^2+Nu^2$, répondent à un groupe particulier de diviseurs linéaires, lesquels pourront toujours être déterminés *a priori*, ainsi qu'on l'a expliqué n°. 301; il convient en même temps de faire entrer dans le développement de ce groupe, non-seulement les nombres impairs, premiers à $N$, mais généralement tous les nombres impairs ou doubles d'un impair donnés par les équations du n°. cité, et même les nombres qui ont un commun diviseur avec $N$, pourvu que ce diviseur ne soit pas un quarré. (Car il faut excepter le cas où les nombres dont il s'agit pourroient être compris parmi les diviseurs de la troisième espèce.) Cela posé, s'il est possible qu'un nombre $c$ pris dans le diviseur $\Delta$ satisfasse à l'équation $c^2=\varphi^2+N\psi^2$, il faudra que le même nombre $c$ appartienne à un diviseur quadratique de forme $Ay^2+Bz^2$ ou $\frac{1}{2}(Ay^2+Bz^2)$, lequel sera également compris dans les diviseurs de première espèce; car le nombre $c$, à raison de sa forme linéaire, ne peut être compris dans aucun autre groupe, que celui qui appartient à la première espèce. Or les seuls diviseurs quadratiques dans lesquels tout nombre compris $c$ satisfait à l'équation $c^2=\varphi^2+N\psi^2$, sont de la forme $Ay^2+Bz^2$ ou de la forme $\frac{1}{2}(Ay^2+Bz^2)$. Il est facile maintenant de séparer parmi les nombres $c$ ceux qui ne sont pas propres à la démonstration.

(323) Dans l'exemple précédent, si l'on considère que le diviseur $225y^2+41z^2$, contient un nombre premier 389 dont le quarré est de la forme $\varphi^2+9225\psi^2$; si l'on considère de même que le diviseur $9y^2+1025z^2$ contient un nombre 1034, double d'un premier, dont le quarré est également de forme $\varphi^2+N\psi^2$, on en conclura que tout nombre $c$ appartenant à l'un ou l'autre diviseur, satisfait à l'équation $c^2=\varphi^2+N\psi^2$. Donc les nombres qui seroient

communs entre le diviseur proposé $189y^2+30yz+50z^2$, et l'un ou l'autre de ces deux derniers diviseurs, doivent être rejetés comme satisfaisant à l'équation $c^2=\varphi^2+N\psi^2$. Or le diviseur $9y^2+1025z^2$ contient les 34 nombres suivans, moindres que $N$, et n'ayant pas de facteur quarré commun avec $N$:

1034, 1061, 1106, 1169, 1349; 1466, 1601, 1754, 2114, 2321; 2546, 2789, 3329, 3626, 3941; 4109, 4181, 4274, 4541, 4829; 4994, 5189, 5381, 5621, 5786; 6209, 6701, 7109, 7349, 7586; 8069, 8081, 8594, 8861.

L'autre diviseur $225y^2+41z^2$ contient pareillement les 29 nombres suivans :

41, 266, 389, 881, 941; 2066, 2189, 2234, 2681, 2849; 2909, 3641, 4034, 4649, 5186; 5609, 5666, 5789, 5861; 6281, 6986, 7154, 7609, 7829; 8141, 8249, 8261, 8561, 8954.

Comparant ces deux suites avec celle des 59 termes qui résultent du diviseur proposé $189y^2+30yz+50z^2$, on trouve qu'il n'y a que sept termes communs, savoir, 2849, 3626, 4181, 5621, 7154, 8249, 8954; lesquels ne sont pas la huitième partie du nombre de toutes les valeurs de $c$ dans le diviseur proposé.

Au reste, quoiqu'il soit probable que le nombre des valeurs communes entre deux diviseurs quadratiques donnés sera toujours très-petit, comme il l'est dans cet exemple, il n'en seroit pas moins utile de déterminer généralement la proportion dans laquelle ces valeurs communes peuvent être avec toutes les valeurs comprises dans chaque diviseur quadratique, et la solution de ce problême particulier contribueroit beaucoup à perfectionner la théorie précédente.

On doit observer à ce sujet que tous les nombres moindres que $N$, compris dans un diviseur proposé $cy^2+2byz+az^2$, seront différens entr'eux, c'est-à-dire que le même nombre ne peut résulter de deux suppositions différentes dans les valeurs de $y$ et $z$. En effet on a prouvé, dans la démonstration du Cas VI, que tous les diviseurs quadratiques $cy^2+2byz+az^2$ qui contiennent le même nombre $c<N$, sont nécessairement différens entr'eux. On peut aussi prouver directement la même proposition pour les diviseurs quadratiques de forme $my^2+nz^2$ (voyez n°. 238); car toutes les

fois qu'un nombre $A$ est contenu de deux manières différentes dans cette formule, il faut, qu'en faisant $n=\alpha\,6$, $m=\gamma\delta$, on ait $4A=(\alpha\gamma B^2+6\delta C^2)(\alpha\delta D^2+6\gamma E^2)$. Or la quantité $f+g$ étant en général plus grande que $2\sqrt{fg}$, on aura $\alpha\gamma B^2+6\delta C^2 > 2BC\sqrt{\alpha 6\gamma\delta}$; par la même raison, l'autre facteur sera $> 2DE\sqrt{\alpha 6\gamma\delta}$, et ainsi on aura $A > BCDE.\alpha 6\gamma\delta$, et à plus forte raison $A > \alpha 6\gamma\delta$ ou $A > N$ (car le diviseur quadratique $my^2+nz^2$ étant supposé appartenir à la formule $t^2+Nu^2$, on a $\alpha 6\gamma\delta = mn = N$). Donc si le nombre $A$ est $< N$, il ne pourra être contenu de deux manières différentes dans la formule $my^2+nz^2$.

(324) Théorème XVII. *Toute formule* $t^2+Nu^2$, *comprise dans les Tables VIII, IX, X et XI, aura nécessairement un ou plusieurs diviseurs quadratiques de première espèce.*

Car suivant le Théorème XIV, la formule $t^2+Nu^2$ aura toujours au moins un diviseur quadratique réciproque; ce diviseur, d'après le Théorème XVI, doit être de la première espèce; donc la formule $t^2+Nu^2$ aura au moins un diviseur de première espèce.

*Remarque.* On voit par les Théorêmes XV, XVI et XVII, que les diviseurs réciproques sont absolument identiques avec ceux de première espèce, et qu'il en existe toujours au moins un dans toute formule $t^2+Nu^2$ de nature à entrer dans les Tables. Il est bon en outre d'observer que la définition des diviseurs réciproques donnée n°. 304, est susceptible d'une plus grande latitude; car il résulte de la démonstration du Théorème XVI, et sur-tout du Cas VI de ce Théorême, qu'un diviseur quadratique de la formule $t^2+Nu^2$ sera réciproque et de première espèce, s'il contient un seul nombre $c$, tel que $N$ divise $t^2+cu^2$, et n'ait en même temps aucun facteur quarré commun avec $c$. D'où l'on voit que les facteurs communs non quarrés entre $c$ et $N$, n'empêchent pas le diviseur dont il s'agit d'être réciproque et de première espèce.

(325) Théorème XVIII. *Si* N *est premier ou double d'un premier, tout diviseur quadratique de la formule* $t^2+Nu^2$, *sera un diviseur de première espèce.*

Car suivant le Théorême XIII, tout diviseur quadratique de la formule

formule $t^2+Nu^2$, est un diviseur réciproque ; et suivant le Théorème XIV, tout diviseur réciproque est de première espèce ; donc si $N$ est premier ou double d'un premier, tout diviseur quadratique de la formule $t^2+cu^2$, c'est-à-dire tout diviseur qui est de nature à entrer dans les Tables VIII, IX, X et XI, ou dans leur prolongement, sera un diviseur de première espèce, et ainsi sera décomposable en trois quarrés.

*Corollaire.* Puisque dans le cas dont il s'agit, chaque diviseur quadratique répond à une forme trinaire de $N$, et ne répond qu'à une seule, il y aura nécessairement autant de diviseurs quadratiques de la formule $t^2+Nu^2$, qu'il y a de formes trinaires du nombre $N$.

(326) Lorsque $N$ est premier ou double d'un premier, la démonstration de la Prop. XVI, sur laquelle celle-ci est appuyée, ne souffre aucune difficulté. En effet, soit $cy^2+2byz+az^2$ un diviseur réciproque proposé de la formule $t^2+Nu^2$, il faudra que $N$ soit diviseur de la formule $t^2+cu^2$; mais par la nature du nombre $c$, il ne peut y avoir qu'un diviseur quadratique de la formule $t^2+cu^2$ qui contienne $N$, et $N$ n'y pourra être contenu que d'une seule manière. Soit donc $k$ le nombre de facteurs premiers impairs et inégaux qui divisent $c$, et il est clair que le nombre $N$ aura, comme diviseur de la formule $t^2+cu^2$, $2^{k-1}$ formes trinaires, lesquelles seront différentes (n°. 288), parce que $N$ plus grand que $c$, est à plus forte raison plus grand que $\frac{4}{3}c$. Cela posé, les $2^{k-1}$ formes trinaires de $N$ feront connoître autant de diviseurs quadratiques de la formule $t^2+Nu^2$, dans chacun desquels $c$ sera contenu; et comme ces diviseurs doivent être différens les uns des autres, puisqu'ils sont correspondans à des valeurs trinaires de $N$ différentes; comme en même temps il ne peut y avoir plus de $2^{k-1}$ diviseurs quadratiques de la formule $t^2+Nu^2$ qui contiennent $c$, il s'ensuit que le diviseur proposé sera nécessairement compris parmi les $2^{k-1}$ diviseurs quadratiques qui répondent aux $2^{k-1}$ valeurs trinaires de $N$. Donc ce diviseur sera de première espèce, ou décomposable en trois quarrés.

La démonstration est, comme on voit, extrêmement simple,

lorsque $N$ est un nombre premier ou double d'un premier, et quoiqu'elle soit toujours appuyée sur les propriétés déjà constatées des formules $t^2+cu^2$ où $c$ est moindre que $N$, elle ne suppose cependant aucun choix dans les valeurs de $c$, et tout nombre compris dans le diviseur proposé $cy^2+2byz+az^2$, pourvu qu'il soit moindre que $N$, peut être pris pour $c$, et conduira toujours à la même conclusion.

Mais comme dans le diviseur proposé il y a toujours un nombre $c$ plus petit que $\sqrt{\frac{4}{3}N}$; si les Tables sont prolongées jusqu'au nombre $c$, la démonstration actuelle, indépendamment de celle qui a été donnée dans le Théorême XVI, étendra la proposition concernant les nombres premiers ou doubles d'un premier jusqu'au nombre $N=\frac{3}{4}c^2$, de sorte qu'en faisant $c=220$, qui est à-peu-près la limite de nos Tables, on aura $N=36300$ pour la limite jusqu'à laquelle le Théorême XVIII est démontré par le seul secours des Tables existantes.

(327) Il seroit à desirer qu'on pût démontrer généralement le Théorême XVIII à l'aide d'une Table particulière qui ne contiendroit que les nombres premiers ou doubles de premiers; mais pour cela, il faudroit prouver que tout diviseur quadratique de la formule $t^2+Nu^2$ (on entend tout diviseur qui est de nature à entrer dans les Tables), contient au moins un nombre, premier ou double d'un premier, moindre que $N$. Or quoique cette proposition soit très-simple en elle-même, très-vraisemblable en général, et déjà constatée dans toute l'étendue des Tables, et beaucoup au-delà, cependant sa démonstration paroît présenter des difficultés. Voici quelques réflexions à ce sujet.

Supposons que la Table qui contient les diviseurs quadratiques de la formule $t^2+cu^2$, pour tout nombre $c$ premier ou double d'un premier, soit continuée jusqu'à la limite $c=36300$, ou telle autre qu'on voudra; ajoutons maintenant au-delà de la limite de la Table la formule immédiatement suivante $t^2+Nu^2$, on pourra, par les méthodes données, chercher tous les diviseurs quadratiques de cette formule, c'est-à-dire tous ceux qui sont de nature à entrer dans la Table (voyez n°. 305); si ces diviseurs sont en nombre

égal avec les formes trinaires du nombre $c$, chaque diviseur quadratique répondra à une valeur trinaire de $c$, et sera également trinaire, ou de première espèce; la Table seroit donc avancée d'une formule de plus, et il n'y auroit rien à démontrer. Si les diviseurs dont il s'agit étoient en moindre nombre que les valeurs trinaires de $c$, il y auroit omission, et en cherchant *a priori* les diviseurs correspondans aux diverses valeurs trinaires de $c$, on en trouveroit autant que de valeurs de $c$, ce qui rétabliroit les diviseurs quadratiques omis; la Table seroit donc encore avancée d'une formule de plus conforme à la loi générale. Il reste enfin à examiner le cas où pour la première fois, dans la construction de la Table, on rencontreroit plus de diviseurs quadratiques de la formule $t^2+Nu^2$, qu'il n'y a de valeurs trinaires de $N$. Alors il faudroit que chaque diviseur qui ne répondroit pas à une valeur trinaire de $N$, ne contînt aucun nombre premier ou double d'un premier moindre que $N$, car s'il en contenoit seulement un, on démontreroit immédiatement que ce diviseur est trinaire, et par conséquent doit coïncider avec l'un de ceux qui correspondent à une valeur trinaire de $N$. Soit $c$ le moindre nombre composé compris dans un de ces diviseurs, $N$ devant être diviseur de $t^2+cu^2$, il faudra donc que les diviseurs réciproques de la formule $t^2+cu^2$ (où $c$ est $<\sqrt{\frac{4}{3}N}$) ne soient pas de première espèce, et ainsi l'infraction à la loi générale se seroit manifestée beaucoup plutôt dans la Table qui comprend les formules $t^2+cu^2$ où $c$ est un nombre quelconque.

Nous ne pousserons pas plus loin ces raisonnemens, qui font assez sentir la nécessité de recourir, comme nous l'avons fait, à la Table générale, au lieu de considérer simplement celle où les nombres $c$ seroient premiers ou doubles de premiers. Nous observerons cependant encore que si par une voie quelconque on pouvoit démontrer directement le Théorême XVIII pour les nombres de l'une des Tables VIII, IX, X et XI, il seroit facile d'étendre la démonstration aux autres Tables. En effet, supposons, par exemple, qu'on a prouvé que les diviseurs quadratiques sont trinaires pour toute formule $t^2+cu^2$ de la Table IX, où $c$ est un nombre premier $8n+3$. Soit proposé ensuite le diviseur quadratique $\alpha y^2+2\varepsilon yz+\gamma z^2$ de

la formule $t^2+2au^2$, où $a$ est un nombre premier. Ce diviseur, soit qu'il se rapporte à la Table X ou à la Table XI, est un diviseur réciproque; et par conséquent $2a$ doit être diviseur de $t^2+Nu^2$, $N$ étant un nombre quelconque compris dans la fonction $\alpha y^2+2\zeta yz+\gamma z^2$. Soit pris parmi les nombres $N$ un nombre premier $c$ de forme $8n+3$, et puisque $2a$ divise $t^2+cu^2$, il faut que $2a$ soit compris dans un diviseur trinaire de cette formule, lequel donnera une valeur trinaire de $2a$. Si ensuite, d'après cette valeur, on cherche le diviseur correspondant de la formule $t^2+2au^2$, ce diviseur contiendra à son tour le nombre premier $c$; il sera donc le même que le diviseur proposé $\alpha y^2+2\zeta yz+\gamma z^2$, d'où il suit que ce dernier est décomposable en trois quarrés.

Un semblable raisonnement, appliqué à la Table VIII, prouvera que les diviseurs quadratiques de toute formule $t^2+cu^2$, où $c$ est un nombre premier de forme $4n+1$, sont trinaires. Car ayant pris dans un de ces diviseurs le nombre $2a$ double d'un premier, il faudra que $c$ divise $t^2+2au^2$. Et cette formule étant contenue dans les Tables X ou XI, on en conclura de même que le diviseur proposé est trinaire.

(328) Le Théorème XVIII étant établi d'une manière quelconque, il est à remarquer qu'on en déduit avec une grande facilité la démonstration du Théorème XVI considéré dans toute sa généralité. En effet, soit $cy^2+2byz+az^2$ un diviseur réciproque proposé de la formule $t^2+Nu^2$, et soit $A$ un nombre premier ou double de premier $>\frac{1}{4}N^2$, contenu dans ce diviseur, il faudra que le nombre $N$ soit diviseur de $t^2+Au^2$, et comme tel contenu dans $2^{i-1}$ diviseurs quadratiques de $t^2+Au^2$. (On désigne toujours par $i$ le nombre de facteurs premiers impairs et inégaux qui divisent $N$.) Ces $2^{i-1}$ diviseurs sont trinaires, puisque $A$ est premier ou double d'un premier; de plus, ils sont tous différens les uns des autres, puisque $N$ est $<\sqrt{\frac{4}{3}A}$, donc le nombre $N$ aura, comme diviseur de la formule $t^2+Au^2$, $2^{i-1}$ valeurs trinaires. Et il importe peu que ces valeurs soient toutes inégales ou qu'il y en ait quelques-unes d'égales, car chaque valeur trinaire de $N$, et la valeur correspondante de $A$, doivent se retrouver ensemble, lorsqu'on consi-

dère à son tour $A$ comme diviseur de $t^2+Nu^2$ (1); d'où il suit que comme les $2^{i-1}$ valeurs trinaires de $A$ sont différentes, il faudra que le diviseur proposé $cy^2+2byz+az^2$ qui contient $A$, réunisse $2^{i-1}$ formes trinaires différentes, conformément à l'énoncé du Théorème XVI.

(329) Théorème XIX. *Tout diviseur quadratique de seconde espèce contenu dans les Tables VIII, IX, X, XI, et dans leur prolongement, est un diviseur non réciproque.*

Soit $py^2+2qyz+rz^2$ un diviseur quadratique de la formule $t^2+cu^2$, lequel, suivant la définition des diviseurs de seconde espèce (n°. 295) ne soit point décomposable en trois quarrés : je dis que ce diviseur sera *non réciproque*, c'est-à-dire que $N$ étant un nombre quelconque premier à $c$, contenu dans ce diviseur, $c$ ne pourra diviser $t^2+Nu^2$. Car soit pris pour $N$ un nombre premier; si on nie la proposition, il faudra que $c$ divise $t^2+Nu^2$, alors $c$ sera contenu dans un diviseur trinaire de la formule $t^2+Nu^2$, puisque celle-ci ne comporte pas d'autre espèce de diviseurs; donc réciproquement $N$ doit être compris dans un diviseur trinaire de la formule $t^2+cu^2$. Mais puisque $N$ est premier, il ne peut y avoir deux diviseurs quadratiques de la formule $t^2+cu^2$ qui contiennent $N$; donc le diviseur proposé $py^2+2qyz+rz^2$ seroit trinaire, ou décomposable en trois quarrés, contre la supposition que ce diviseur est non décomposable. Donc on ne peut supposer que $c$ divise $t^2+Nu^2$; donc tout diviseur quadratique de seconde espèce est un diviseur non réciproque.

*Remarque.* Tout diviseur de seconde espèce, relatif à la formule $t^2+cu^2$, est non-réciproque, même pour les nombres contenus qui ont un commun diviseur avec $c$; c'est-à-dire que si $N$ est un nombre contenu dans le diviseur dont il s'agit, quand même $N$ et $c$ auroient un commun diviseur, $c$ ne pourra diviser $t^2+Nu^2$.

(1) Cette observation, appliquée à la démonstration du Théorème XVI, peut servir à lever toute difficulté dans le cas où on a $c^2=q^2+N\psi^2$. C'est ce qui sera développé ci-après dans les supplémens.

Il faut excepter seulement le cas où $N$ est multiple de $c$, car alors il est évident que $c$ divisera toujours $t^2+Nu^2$.

(330) THÉORÈME XX. *Tout diviseur quadratique non réciproque ne sauroit être trinaire, à moins qu'il ne se rapporte à la troisième espèce.*

Car un diviseur quadratique non réciproque ne peut être de la première espèce, suivant le Théorème XV; il ne peut être non plus de la seconde espèce, s'il est décomposable en trois quarrés; puisque les diviseurs de cette espèce ont pour caractère de n'être point décomposables; donc les diviseurs, qui sont à-la-fois non réciproques et trinaires, ne peuvent être relatifs qu'à la troisième espèce. Ces diviseurs sont réciproques par rapport aux nombres compris qui ont un facteur quarré commun avec les trois termes de la valeur correspondante de $c$; ils sont *non réciproques* par rapport à tous les autres nombres.

(331) THÉORÈME XXI. *Tout nombre impair, excepté seulement les nombres $8n+7$, est la somme de trois quarrés.*

Cette proposition est maintenant un corollaire très-simple de la théorie précédente. Car tout nombre impair $c$ qui n'est pas de la forme $8n+7$, sera soit de la forme $4n+1$, soit de la forme $8n+3$; la formule $t^2+cu^2$ se rencontrera donc, soit dans la Table VIII, soit dans la Table IX. Mais il a été démontré (Théorême XIV) que toute formule prise dans ces Tables doit avoir au moins un diviseur quadratique réciproque, et ensuite par le Théorême XVI on a fait voir que ce diviseur est de première espèce, et qu'ainsi il y a au moins une valeur correspondante de $c$, exprimée par la somme de trois quarrés. Donc tout nombre impair de la forme $4n+1$, ou de la forme $8n+3$, est la somme de trois quarrés.

*Il résulte en même temps de la théorie précédente, que quand même le nombre* c *seroit divisible par un quarré, on pourra toujours supposer que les trois quarrés composant la valeur de* c *ne sont pas divisibles par un même nombre.*

C'est ainsi qu'on a $81=8^2+4^2+1^2$, $225=14^2+5^2+2^2$, et ainsi des autres. D'où l'on voit que chaque nombre $4n+1$ ou $8n+3$,

a tout au moins une valeur trinaire qui lui est propre, et qui est indépendante de celles des nombres inférieurs.

*Corollaire.* De ce que tout nombre $8n+3$ est de la forme $p^2+q^2+r^2$, il s'ensuit (n°. 155) que *tout nombre entier est la somme de trois triangulaires*, ce qui est le fameux théorême de Fermat dont nous avons déjà parlé.

(332) Théorème XXII. *Tout nombre double d'un impair est la somme de trois quarrés.*

C'est encore une conséquence immédiate des Théorêmes XIV et XVI appliqués aux Tables X et XI. Et on voit de plus par cette théorie, que quand même le nombre dont il s'agit seroit divisible par un quarré, on pourra toujours en avoir une valeur exprimée par trois quarrés qui n'auront pas de commun diviseur.

*Corollaire I.* Un nombre quelconque double d'un impair, étant désigné par $4a+2$, on pourra toujours satisfaire à l'équation $4a+2=x^2+y^2+z^2$. Or par la forme du premier membre, on voit que deux des nombres $x$, $y$, $z$ doivent être impairs et le troisième pair, on peut donc faire $x=p+q$, $y=p-q$, $z=2r$, et on aura $2a+1=p^2+q^2+2r^2$; donc *tout nombre impair est de la forme* $p^2+q^2+2r^2$.

Cette proposition avoit été avancée par *Fermat*, comme étant particulière aux nombres premiers $8n+7$; mais on voit qu'elle s'étend généralement à tous les nombres impairs; et on sait de plus, par la théorie précédente, que dans le cas où le nombre proposé $2a+1$ seroit divisible par un quarré, il est toujours possible de trouver pour ce nombre une forme $p^2+q^2+2r^2$, telle que ses trois termes ne soient pas divisibles par un même facteur; c'est-à-dire qu'en général on peut satisfaire à l'équation $(2b+1)k^2=x^2+y^2+2z^2$, sans supposer que $x$, $y$, $z$ aient un diviseur commun.

*Corollaire II.* Un nombre entier quelconque peut toujours être représenté par l'une des formules $(2a+1)2^{2m}$, $(4a+2)2^{2m}$; or s'il appartient à la première, il sera, suivant ce qu'on vient de démontrer, de la forme $p^2+q^2+2r^2$, et s'il appartient à la seconde formule, il sera de la forme $p^2+q^2+r^2$. Donc *tout nombre entier, ou au moins son double, est la somme de trois quarrés.*

(333) Théorème XXIII. *Soit* N *un nombre quelconque de l'une des formes* $4n+1$, $8n+3$, $4n+2$, *lesquelles comprennent tous les nombres impairs et doubles d'un impair, excepté seulement les nombres* $8n+7$; *si on désigne par* i *le nombre de facteurs premiers impairs et inégaux qui divisent* N, *je dis que le nombre* N *aura au moins* $2^{i-2}$ *formes trinaires différentes.*

Car dans ces différens cas, la formule $t^2+Nu^2$ appartiendra à l'une des Tables VIII, IX, X, XI : or on a prouvé que toute formule comprise dans ces Tables doit avoir au moins un diviseur quadratique de première espèce. On a prouvé en même temps que ce diviseur se décompose en $2^{i-1}$ formes trinaires différentes, dont chacune répond à une valeur trinaire de $N$, et quant à ces valeurs, il ne peut arriver que deux cas ; ou elles sont toutes inégales entre elles, et alors leur nombre est $2^{i-1}$; ou elles sont égales deux à deux (ce qui a lieu lorsque le diviseur est de l'une des formes $cy^2+az^2$, $cy^2+2byz+2bz^2$, $cy^2+2byz+cz^2$, et qu'en même temps le moindre des coefficiens extrêmes n'est ni 1 ni 2), et alors le nombre des valeurs inégales de $N$ est $2^{i-2}$. Donc dans tous les cas le nombre $N$ aura au moins $2^{i-2}$ formes trinaires de première espèce, ou dont les trois termes ne sont pas divisibles par un même facteur.

Ainsi le nombre 3.5.7.11.13.17.19, composé de sept facteurs inégaux, et qui, comme on le voit aisément, est de forme $8n+5$, doit avoir au moins $2^5$ ou 32 formes trinaires différentes. Il peut aussi en avoir un beaucoup plus grand nombre ; et c'est ce qu'on détermineroit exactement, en cherchant le nombre de diviseurs de première espèce qui conviennent à la formule $t^2+Nu^2$, pour cette valeur particulière de $N$.

De-là on voit qu'il est facile de trouver un nombre qui ait tant de formes trinaires qu'on voudra ; problême analogue à celui du n°. 237.

QUATRIÈME

# QUATRIÈME PARTIE.

## *MÉTHODES ET RECHERCHES DIVERSES.*

### §. I. *Théorèmes sur les puissances des Nombres.*

La méthode dont nous allons donner diverses applications, mérite une attention particulière, en ce qu'elle est jusqu'à présent la seule par laquelle on ait pu démontrer certaines propositions négatives sur les puissances des nombres. Le but de cette méthode est de faire voir que si la propriété dont on nie l'existence avoit lieu pour de grands nombres, elle auroit lieu également pour des nombres plus petits. Ce premier point étant établi, la proposition est démontrée, car pour que le contraire eût lieu, il faudroit qu'une suite de nombres entiers décroissans pût être prolongée à l'infini, ce qui implique contradiction. Fermat est le premier qui ait indiqué cette méthode dans une de ses notes sur Diophante, où il prouve que l'aire d'un triangle rectangle en nombres entiers (1) ne sauroit être égale à un quarré. Euler en a depuis étendu les applications, et l'a exposée avec beaucoup de clarté dans le Tom. II de ses Élémens d'Algèbre.

(334) Théorème I. *L'aire d'un triangle rectangle en nombres entiers ne sauroit être égale à un quarré.*

Puisqu'on a $(a^2+b^2)^2=(a^2-b^2)^2+(2ab)^2$, il est clair que les trois côtés d'un triangle rectangle peuvent être représentés par les nombres $a^2+b^2$, $a^2-b^2$, $2ab$; c'est aussi l'expression générale qu'on déduiroit de la résolution directe de l'équation $x^2=y^2+z^2$

(1) Trois nombres tels que le quarré du plus grand équivaut à la somme des quarrés des deux autres, sont ce qu'on appelle un *triangle rectangle*. On peut donner pour exemple les nombres 3, 4, 5, les nombres 5, 12, 13, et une infinité d'autres.

(n°. 17). Ces trois nombres pourroient de plus être multipliés par un facteur commun $\theta$ ; mais nous ferons abstraction de ce facteur, qui est inutile pour notre objet, et par la même raison, nous supposerons $a$ et $b$ premiers entr'eux. En effet, si les trois côtés d'un triangle sont divisibles par $\theta$, l'aire sera divisible par $\theta^4$ ; donc si cette aire est un quarré, elle le sera encore après avoir été divisée par son facteur $\theta^4$.

Cela posé, appelons $\mathcal{A}$ l'aire du triangle dont il s'agit, nous aurons $\mathcal{A}=ab(a^2-b^2)$ ; et comme les facteurs $a$ et $b$ sont premiers entr'eux, ils le seront également avec $a^2-b^2$ ; donc pour que $\mathcal{A}$ soit un quarré, il faut que chacun des facteurs $a$, $b$, $a^2-b^2$ en soit un. Soit donc $a=m^2$, $b=n^2$, il restera à faire en sorte que $a^2-b^2$ ou $m^4-n^4$ soit égal à un quarré.

Cette quantité $m^4-n^4$ est le produit des deux facteurs $m^2+n^2$, $m^2-n^2$ : or $m$ et $n$ sont premiers entr'eux, puisque $a$ et $b$ le sont. De plus, ils doivent être supposés l'un pair et l'autre impair ; car s'ils étoient impairs tous deux, $a$ et $b$ le seroient aussi, et ainsi les trois côtés $a^2+b^2$, $a^2-b^2$, $2ab$ seroient divisibles par 2, ce qui est contre la supposition. Donc les facteurs $m^2+n^2$ et $m^2-n^2$ sont premiers entr'eux ; et puisque leur produit doit être un quarré, il faudra que chacun d'eux en soit un.

Faisons en conséquence $m^2+n^2=p^2$, $m^2-n^2=q^2$, nous aurons $n^2+q^2=m^2$, et $2n^2+q^2=p^2$. Donc *si l'aire d'un triangle rectangle est un quarré, on pourra trouver deux quarrés* $q^2$, $n^2$, *tels que chacune des deux quantités* $q^2+n^2$, $q^2+2n^2$ *soit égale à un quarré* (1).

---

(1) Voici le passage de Fermat que nous suivons assez strictement, en ajoutant seulement les développemens nécessaires pour rendre la démonstration plus claire et plus complète :

« Si area trianguli esset quadratus darentur duo quadrato-quadrati quorum » differentia esset quadratus : Unde sequitur dari duo quadrata quorum et summa » et differentia esset quadratus. Datur itaque numerus compositus ex quadrato et » duplo quadrati æqualis quadrato, ea conditione ut quadrati eum componentes » faciant quadratum. Sed si numerus quadratus componitur ex quadrato et duplo » alterius quadrati, ejus latus similiter componitur ex quadrato et duplo quadrati, » ut facillime possumus demonstrare.

» Unde concluditur latus illud esse summam laterum circa rectum trianguli rec-

Puisqu'on a $p^2 = q^2 + 2n^2$, il faut (n°. 141) que $p$ soit de la forme $f^2 + 2g^2$ : or on satisfait à l'équation $q^2 + 2n^2 = (f^2 + 2g^2)^2$ en faisant $q + n\sqrt{-2} = (f + g\sqrt{-2})^2$, ce qui donne

$$q = f^2 - 2g^2$$
$$n = 2fg;$$

et cette solution est d'ailleurs aussi complète qu'on peut le desirer, comme on peut s'en assurer par les formules du n°. 17. Il reste donc à satisfaire à l'équation $q^2 + n^2 = m^2$, dans laquelle substituant les valeurs trouvées pour $q$ et $n$, on aura $f^4 + 4g^4 = m^2$.

Cette dernière équation, qui doit être possible si l'aire $A$ est un quarré, présente un nouveau triangle rectangle formé avec l'hypothénuse $m$ et les deux côtés $f^2$, $2g^2$ : or l'aire de ce triangle étant $f^2g^2$, et par conséquent égale à un quarré, il s'ensuit que si l'aire $A$ du triangle rectangle proposé est égale à un quarré, on pourra, par le moyen de ce triangle, en découvrir un beaucoup plus petit, mais non pas nul, dont l'aire sera pareillement égale à un quarré.

(335) Pour juger de la petitesse de ce second triangle rectangle en comparaison du premier, il faut exprimer la valeur de $A$ en $f$ et $g$: or on trouve

$$A = (m^4 - n^4)m^2n^2 = 4f^2g^2(f^2 - 2g^2)^2(f^2 + 2g^2)^2(f^4 + 4g^4).$$

D'ailleurs $f^2 - 2g^2$ ne peut être moindre que 1, et on a toujours $(f^2 + 2g^2)^2 > 8f^2g^2$, $f^4 + 4g^4 > 4f^2g^2$; donc l'aire $A$ est plus grande

---

» tanguli et unum ex quadratis illud componentibus efficere basem et duplum quadratum æquari perpendiculo.

» Illud itaque triangulum rectangulum conficietur a duobus quadratis quorum summa et differentia erunt quadrati. At isti duo quadrati minores probabuntur primis quadratis suppositis quorum tam summa quam differentia faciunt quadratum. Ergo si dentur duo quadrata quorum summa et differentia faciunt quadratum, dabitur in integris summa duorum quadratorum ejusdem naturæ priore minor. Eodem ratiocinio dabitur et minor ista inventa per viam prioris et semper in infinitum minores invenientur numeri in integris idem præstantes : quod impossibile est, quia dato numero quovis integro non possunt dari infiniti in integris illo minores ». Ed. cit. de Dioph. pag. 339.

que $128 f^8 g^8$ ; donc $f^2 g^2$, qui est l'aire du second triangle, étant nommée $A'$, on aura $A' < \sqrt[3]{\frac{A}{128}}$.

De-là on voit que s'il existe un triangle rectangle en nombres entiers, dont l'aire $A$ soit égale à un quarré, il existera en même temps un triangle rectangle dont l'aire $A'$, plus petite que $\sqrt[3]{\frac{A}{128}}$, sera encore égale à un quarré, et cependant ne sera pas nulle, car l'un des nombres $f$ et $g$ ne peut être nul sans rendre $A = 0$.

Mais par la même raison, du triangle rectangle dont l'aire $A'$ est égale à un quarré, on pourra déduire un troisième triangle dont l'aire $A''$, plus petite que $\sqrt[3]{\frac{A'}{128}}$, sera égale à un quarré, et ainsi à l'infini. Or il implique contradiction qu'une suite de nombres entiers $A$, $A'$, $A''$, &c., quand même ils ne seroient pas quarrés, soit décroissante et prolongée à l'infini. Donc il n'existe aucun triangle rectangle dont l'aire soit égale à un quarré.

*Corollaire.* La même démonstration prouve que la formule $m^4 - n^4$ ne peut être un quarré, non plus que la formule $f^4 + 4g^4$, excepté seulement dans les cas évidens, l'un de $m = n$, ou $n = 0$; l'autre de $f$ ou $g = 0$.

On peut aussi en conclure que l'équation $x^4 + y^4 = 2p^2$ est impossible, hors le cas de $x = y$; car de cette équation on tireroit $p^4 - x^4 y^4 = \left(\frac{x^4 - y^4}{2}\right)^2$; or on vient de voir que le premier membre ne peut être un quarré.

(336) THÉORÈME II. *La somme de deux biquarrés ne peut être égale à un quarré, à moins que l'un d'eux ne soit nul.*

Soit, s'il est possible, $a^4 + b^4 = c^2$; il faudra d'abord qu'on ait $a^2 = p^2 - q^2$, $b^2 = 2pq$, $c = p^2 + q^2$. J'observe ensuite que $a$ et $b$ pouvant être supposés premiers entr'eux, $p$ et $q$ seront pareillement premiers entr'eux, et même ils ne pourront être tous deux impairs; car s'ils l'étoient, $a$ et $b$ seroient tous deux pairs. On ne pourra non plus supposer $p$ pair et $q$ impair, parce qu'alors $p^2 - q^2$ seroit de la forme $4k - 1$, laquelle ne peut convenir au quarré $a^2$. Donc il faudra que $p$ soit impair et $q$ pair, et ainsi, pour satisfaire

à l'équation $b^2 = 2pq$, on prendra $p = m^2$, $q = 2n^2$, valeurs qui étant substituées dans l'autre équation $a^2 = p^2 - q^2$, donneront $m^4 - 4n^4 = a^2$.

Cette dernière équation exprimant que le quarré $m^4$ est égal à la somme de deux autres quarrés $4n^4$, $a^2$, le seul moyen d'y satisfaire est de prendre $m^2 = f^2 + g^2$, $2n^2 = 2fg$, $a = f^2 - g^2$. Or l'équation $n^2 = fg$ où $f$ et $g$ doivent être premiers entr'eux, donne $f = \alpha^2$, $g = \zeta^2$, et par ces valeurs, l'équation $m^2 = f^2 + g^2$ devient $\alpha^4 + \zeta^4 = m^2$.

D'où l'on voit que s'il existe deux biquarrés $a^4$, $b^4$ dont la somme soit égale à un quarré $c^2$, il existera en même temps deux autres biquarrés beaucoup plus petits $\alpha^4$, $\zeta^4$ dont la somme sera pareillement égale à un quarré.

(337) Et pour rendre sensible la petitesse de ceux-ci en comparaison des premiers, on déduira des valeurs précédentes,

$$a = \alpha^4 - \zeta^4$$
$$b = 2\alpha\zeta\sqrt{(\alpha^4 + \zeta^4)};$$

ce qui donne $\alpha^4 + \zeta^4 = \sqrt{[\frac{1}{2}a^2 + \frac{1}{2}\sqrt{(a^4 + b^4)}]}$, et par conséquent $\alpha^4 + \zeta^4 < \sqrt[4]{(a^4 + b^4)}$. On remarquera d'ailleurs que $\alpha$ ni $\zeta$ ne peuvent être zéro, parce qu'il s'ensuivroit $b = 0$, cas exclu.

S'il existe donc un quarré $c^2$ égal à la somme de deux biquarrés, on connoîtra par son moyen un second quarré $c'^2$, pareillement égal à la somme de deux biquarrés, et dont le côté $c'$ sera $< \sqrt[4]{c}$, sans être nul ; mais par la même raison, le quarré $c'^2$ en fera connoître un troisième $c''^2$ jouissant de la même propriété, et dont le côté $c''$ sera $< \sqrt[4]{c'}$ sans être nul ; ainsi de suite. Or il implique contradiction qu'une suite de nombres entiers $c$, $c'$, $c''$, &c. dont chacun est plus petit que la racine quatrième du précédent, sans être nul, puisse être prolongée à l'infini. Donc il est impossible qu'un quarré se décompose en deux biquarrés.

*Corollaire.* La même démonstration prouve que la formule $m^4 - 4n^4$ ne peut être égale à un quarré, si ce n'est lorsque $n = 0$.

(338) THÉORÈME III. *La formule* $x^4 + 2y^4$ *ne peut être égale à un quarré, si ce n'est lorsque* $y = 0$.

Car si l'on fait $x^4 + 2y^4 = z^2$, il faudra d'abord supposer $z = p^2 + 2q^2$,

$x^2=p^2-2q^2$, $y^2=2pq$; ensuite l'équation $x^2=p^2-2q^2$ donnera $x=m^2-2n^2$; $p=m^2+2n^2$, $q=2mn$. Ces valeurs étant substituées dans l'équation $y^2=2pq$, on aura $y^2=4mn(m^2+2n^2)$. Pour satisfaire à cette dernière équation, j'observe que les nombres $m$ et $n$ sont premiers entr'eux; car s'ils avoient un commun diviseur, $p$ et $q$ en auroient un aussi, et par suite $x$ et $y$, ce qu'on doit ne pas supposer. Donc si $mn(m^2+2n^2)$ est un quarré, il faudra que ses trois facteurs $m$, $n$, $m^2+2n^2$ soient chacun un quarré. Soit donc $m=f^2$, $n=g^2$, et il restera à faire en sorte que $f^4+2g^4$ soit égale à un quarré.

Cette formule est semblable à la proposée, et il est visible qu'elle est exprimée en nombres beaucoup plus petits, car on a $x^4+2y^4>p^4$, et par conséquent $p$ ou $f^4+\sqrt[4]{2g^4}<(x^4+2y^4)$; d'ailleurs les nombres $f$ et $g$ ne sont nuls, ni l'un ni l'autre, puisque s'ils l'étoient, ils rendroient $y$ nul, ce qui est un cas dont on fait abstraction. De-là il suit qne si on a un quarré $A^2$ qui soit de la forme $x^4+2y^4$, on pourra en déduire un second quarré $A'^2$ qui sera de la même forme, et dont le côté $A'$ sera $<\sqrt[4]{A}$: mais par la même raison le quarré $A'^2$ en fera connoître un troisième $A''^2$ de même forme, et ainsi de suite. Or il est impossible qu'une suite de nombres entiers $A$, $A'$, $A''$, &c. soit décroissante et prolongée à l'infini; donc il est impossible que la formule $x^4+2y^4$ soit un quarré, à moins qu'on n'ait $y=0$.

*Corollaire.* Il suit de cette proposition, que la formule $x^4-8y^4$ ne peut non plus être égale à un quarré; car si on avoit $x^4-8y^4=z^2$, il s'ensuivroit que $z^4+2(2xy)^4$ est égale au quarré $(x^4+8y^4)^2$, ce qui ne peut avoir lieu que lorsque $y=0$.

(339) Théorème IV. *Aucun nombre triangulaire, excepté l'unité, n'est égal à un biquarré.*

Soit, s'il est possible, $\frac{1}{2}x(x+1)=y^4$, ou $x(x+1)=2y^4$; si l'on fait $y=mn$, $m$ et $n$ étant deux indéterminées, cette équation ne pourra se décomposer que de l'une de ces deux manières:

$$\left.\begin{array}{r}x=2m^4\\ x+1=n^4\end{array}\right\}(1)\qquad\qquad \left.\begin{array}{r}x+1=2m^4\\ x=n^4\end{array}\right\}(2),$$

lesquelles donnent soit $1=n^4-2m^4$, soit $1=2m^4-n^4$.

La seconde combinaison donneroit $m^8 - n^4 = (m^4 - 1)^2$, équation impossible, parce que le premier membre est de la forme $p^4 - q^4$, laquelle ne peut être un quarré, que dans le cas évident de $m = 1 = x$.

La première combinaison donne $1 + 2m^4 = n^4$, équation également impossible, parce qu'en vertu du Théorème précédent, le premier membre ne peut être un quarré. Donc aucun nombre triangulaire, excepté 1, n'est égal à un biquarré.

(340) Théorème V. *La somme ou la différence de deux cubes ne peut être égale à un cube.*

Soit, s'il est possible, $x^3 \pm y^3 = z^3$, on pourra supposer à l'ordinaire que les deux nombres $x$ et $y$ sont premiers entr'eux, et alors $y$ et $z$ seront également premiers entr'eux, ainsi que $x$ et $z$. Cela posé, des trois nombres $x, y, z$, il y en aura toujours deux impairs et un pair; soient $x$ et $y$ les deux impairs, qu'on peut toujours placer dans un même membre; si l'on fait $x \pm y = 2p$, $x \mp y = 2q$, ou bien $x = p + q$, $\pm y = p - q$, on aura par la substitution $2p(p^2 + 3q^2) = z^3$; et on observera ultérieurement, que puisque $p+q$ et $p-q$ doivent être impairs, il faut que $p$ et $q$ soient l'un pair, l'autre impair; de sorte que $p^2 + 3q^2$ sera toujours impair. Mais $2p(p^2 + 3q^2)$ devant être un cube, il est clair que $2p$ sera divisible par 8, et ainsi $p$ sera pair et $q$ impair. Maintenant il y a deux cas à distinguer, selon que $p$ est ou n'est pas divisible par 3.

(341) *Premier Cas.* Si $p$ n'est pas divisible par 3, les facteurs $2p$, $p^2 + 3q^2$ seront premiers entr'eux, et si leur produit est un cube, il faudra que chacun d'eux en soit un. Soit donc $p^2 + 3q^2 = r^3$, alors $r$ sera de la forme $m^2 + 3n^2$, et on pourra faire $p + q\sqrt{-3} = (m + n\sqrt{-3})^3$, ce qui donnera

$$p = m^3 - 9mn^2$$
$$q = 3m^2n - 3n^3.$$

Ces valeurs satisfont à l'équation $p^2 + 3q^2 = r^3$, mais d'ailleurs elles ont toute la généralité nécessaire, ainsi qu'on peut s'en assurer par la résolution directe de cette équation. Il ne reste donc plus qu'à faire en sorte que $2p$ ou $2m(m + 3n)(m - 3n)$ soit un cube.

Or il est aisé de voir que les trois facteurs de cette quantité sont premiers entr'eux, et ainsi chacun d'eux doit être un cube ; soit en conséquence $m+3n=a^3$, $m-3n=b^3$, $2m=c^3$, on aura $a^3+b^3=c^3$. De-là on voit que si l'équation $x^3\pm y^3=z^3$ est possible en nombres entiers, l'équation $a^3+b^3=c^3$ semblable à la première et exprimée en nombres beaucoup plus petits, sera également possible.

Soit $A=x^3\pm y^3=2p(p^2+3q^2)$, et $A'=a^3+b^3$, on aura par la substitution des valeurs précédentes,

$$A=(a^3+b^3)a^3b^3\left(\frac{a^6+a^3b^3+b^6}{3}\right)^3,$$

et à cause de $a^6+b^6>2a^3b^3$, cette formule donnera $A>(a^3+b^3)a^{12}b^{12}$. Mais (excepté dans le cas de $a=b=1$ qui ne peut jamais avoir lieu) on a toujours $a^3b^3>\frac{a^3+b^3}{2}$; donc $\frac{A}{2}$ est plus grand que $\left(\frac{a^3+b^3}{2}\right)^5$ ou $\left(\frac{A'}{2}\right)^5$; donc $\frac{A'}{2}<\sqrt[3]{\frac{A}{2}}$. Mais par le même raisonnement on déduiroit du cube $A'$ un troisième cube $A''$ tel que $\frac{1}{2}A''$ seroit $<\sqrt[3]{\frac{1}{2}A'}$, et ainsi à l'infini : or il est impossible qu'une suite de nombres entiers $A$, $A'$, $A''$, &c. soit décroissante et prolongée à l'infini ; donc il est impossible que la formule $2p(p^2+3q^2)$ soit un cube, au moins lorsque $p$ n'est pas divisible par 3.

(342) *Second Cas.* Si $p$ est divisible par 3, on fera $p=3r$, et la formule $2p(p^2+3q^2)$ deviendra $18r(q^2+3r^2)$. Maintenant comme les facteurs $18r$, $q^2+3r^2$ sont premiers entr'eux, il faudra que chacun d'eux soit un cube. Faisant donc d'abord $q^2+3r^2=(f^2+3g^2)^3$, ou plutôt $q+r\sqrt{-3}=(f+g\sqrt{-3})^3$, ce qui donnera

$$q=f^3-9fg^2$$
$$r=3f^2g-3g^3,$$

il restera à faire en sorte que $18r$ ou $27\cdot 2g(f+g)(f-g)$ soit un cube. De-là on déduira comme ci-dessus $f+g=a^3$, $f-g=b^3$, $2g=c^3$, et par conséquent $a^3+b^3=c^3$. Or on fera voir de même que le cube $c^3$ égal à $a^3+b^3$, est beaucoup plus petit que le cube $z^3$ égal à $2p(p^2+3q^2)$ ; on retombera donc encore sur une suite de nombres entiers qui devroit être décroissante et prolongée à l'infini ; d'où

d'où l'on conclura que l'équation $x^3 \pm y^3 = z^3$ est impossible, à moins que l'un des termes ne soit zéro.

(343) THÉORÈME VI. *La somme ou la différence de deux cubes inégaux ne peut être double d'un cube.*

Soit, s'il est possible, $x^3 \pm y^3 = 2z^3$, les nombres $x$ et $y$ qu'on peut supposer premiers entr'eux seront tous deux impairs; ainsi on pourra faire $x = p+q$, $\pm y = p-q$, ce qui donnera $p(p^2+3q^2) = z^3$, et il faudra distinguer deux cas, selon que $p$ est ou n'est pas divisible par 3.

1°. Si $p$ n'est pas divisible par 3, les deux facteurs $p$, $p^2+3q^2$ seront premiers entr'eux, ainsi il faudra que chacun d'eux soit un cube. Or en faisant $p^2+3q^2 = (m^2+3n^2)^3$, ou plutôt $p+q\sqrt{-3} = (m+n\sqrt{-3})^3$, on aura comme ci-dessus, $p = m^3 - 9mn^2 = m(m+3n)(m-3n)$. Donc puisque ce produit est un cube, et que ses trois facteurs sont premiers entr'eux, il faudra faire $m+3n = a^3$, $m-3n = b^3$, $m = c^3$, ce qni donnera $a^3+b^3 = 2c^3$, équation semblable à la proposée, mais exprimée en nombres beaucoup plus petits.

2°. Si $p$ est divisible par 3, soit $p = 3r$, on aura $9r(3r^2+q^2) = z^3$, de sorte que $9r$ doit être un cube aussi bien que $3r^2+q^2$. Celui-ci devient un cube en faisant $q+r\sqrt{-3} = (m+n\sqrt{-3})^3$, ce qui donne $r = 3m^2n - 3n^3$, partant $9r = 27n(m+n)(m-n)$. Cette quantité devant être un cube, on fera comme ci-dessus $m+n = a^3$, $m-n = b^3$, $n = c^3$, ce qui donnera de nouveau $a^3+b^3 = 2c^3$; équation encore semblable à la proposée, mais exprimée en nombres beaucoup plus petits.

De-là on conclura, comme dans les théorêmes précédens, que l'équation proposée $x^3 \pm y^3 = 2z^3$ est impossible, à moins que $x$ ne soit égal à $y$.

(344) THÉORÈME VII. *Aucun nombre triangulaire, excepté 1, n'est égal à un cube.*

Car supposons pour un moment qu'on ait $\frac{1}{2}x(x+1) = y^3$, ou $x(x+1) = 2y^3$; si on fait $y = mn$, $m$ et $n$ étant deux indétermi-

nées, cette équation ne pourra se décomposer que de l'une de ces deux manières :

$$\left.\begin{array}{r} 1+x=2m^3 \\ x=\ \ n^3 \end{array}\right\}(1) \qquad \left.\begin{array}{r} 1+x=\ \ n^3 \\ x=2m^3 \end{array}\right\}(2),$$

lesquelles donnent $n^3 \pm 1 = 2m^3$. Mais suivant le théorême précédent, cette équation ne peut avoir lieu, à moins qu'on n'ait $n=1$, donc, excepté les cas de $x=0$ et $x=1$, il ne peut y avoir aucun nombre triangulaire égal à un cube.

*Corollaire.* L'équation $\frac{1}{2}x(x+1)=y^3$, peut être mise sous la forme $8y^3+1=z^2$; donc celle-ci n'est possible que pour les seuls cas de $y=0$ et $y=1$.

*Remarque.* Nous avons démontré dans ce paragraphe, que l'équation $x^3 \pm y^3 = z^3$ est impossible, ainsi que l'équation $x^4 \pm y^4 = z^2$, et à plus forte raison $x^4 \pm y^4 = z^4$. Fermat a assuré de plus (Ed. cit. de Dioph. pag. 61) que l'équation $x^n + y^n = z^n$, est généralement impossible, lorsque $n$ surpasse 2; mais cette proposition, passé le cas de $n=4$, est du nombre de celles qui restent à démontrer, et pour lesquelles les méthodes que nous venons d'exposer paroissent insuffisantes. Au reste, il est aisé de voir que la proposition seroit démontrée en général, si elle l'étoit pour le cas où $n$ est un nombre premier.

---

## §. II. *Théorèmes concernant la résolution en nombres entiers de l'équation* $x^n - b = ay$.

(345) Si l'on satisfait à l'équation proposée en faisant $x = \theta$, on y satisfera plus généralement, en faisant $x = \theta + az$, $z$ étant un nombre indéterminé. Or dans la suite formée d'après le terme général $\theta + az$, il y aura toujours un terme compris entre $-\frac{1}{2}\theta$ et $\frac{1}{2}\theta$; on peut donc regarder ce terme comme une *solution* ou *racine* de l'équation proposée; et la question est de trouver toutes les solutions ou racines de cette sorte dont l'équation proposée est susceptible. Voici différens Théorêmes qui remplissent cet objet dans le cas où $a$ est un nombre premier; nous considérerons ensuite le cas où $a$ est un nombre composé.

(346) Théorème I. *L'équation* $\frac{x^n - b}{a} = e$, *dans laquelle* a *est un nombre premier*, *et* b *un nombre non divisible par* a, *ne sera possible qu'autant qu'on aura* $\frac{b^{\frac{a-1}{\omega}} - 1}{a} = e$, $\omega$ *étant le commun diviseur de* n *et de* $a - 1$. *Si cette condition est remplie, l'équation proposée aura un nombre* $\omega$ *de solutions qui seront comprises dans l'équation* $\frac{x^\omega - b^\pi}{a} = e$, *où* $\pi$ *est le moindre entier positif qui satisfait à l'équation* $\pi n - \phi(a-1) = \omega$.

Si l'équation proposée est résoluble, on aura, en rejetant les multiples de $a$, $x^n = b$; on a en même temps, par le Théorême de Fermat (n°. 129) $x^{a-1} = 1$. Les deux nombres $n$ et $a - 1$ ayant pour commun diviseur $\omega$, si l'on fait $n = n'\omega$, $a - 1 = a'\omega$, il sera facile de trouver deux autres nombres positifs $\pi$ et $\phi$ tels qu'on ait

$$\pi n' - \phi a' = 1.$$

Maintenant des équations $x^{n'\omega} = b$, $x^{a'\omega} = 1$, on tire $b^\pi = x^{\pi n'\omega} = x^{\phi a'\omega + \omega} = x^\omega$, donc $x^\omega = b^\pi$, ou

$$\frac{x^\omega - b^\pi}{a} = e;$$

d'où l'on voit que l'équation proposée ne pourra avoir qu'un nombre $\omega$ de solutions (n°. 132); et pour qu'elle ait effectivement ces solutions, il faudra que les deux équations $x^{n'\omega}=b$, $x^{a'\omega}=1$ puissent s'accorder entr'elles. Or ces dernières donnent $x^{n'a'\omega}=b^{a'}$, $x^{n'a'\omega}=1^{n'}=1$; donc il faudra qu'on ait $b^{a'}=1$, ou

$$\frac{b^{a'}-1}{a}=e.$$

Cette condition est la seule nécessaire, et toutes les fois qu'elle sera remplie, l'équation proposée aura un nombre $\omega$ de solutions contenues dans l'équation $\frac{x^{\omega}-b^{\pi}}{a}=e$. Or on s'assure que celle-ci a effectivement un nombre $\omega$ de solutions, en observant que $x^{\omega}-b^{\pi}$ est facteur de $x^{a'\omega}-b^{a'\pi}$ qui revient à $x^{a-1}-1+aR$.

Remarquez que si dans l'équation proposée $n$ est plus grand que $a-1$, on peut ôter de cet exposant les multiples de $a-1$, et ne conserver que le reste positif. En effet $x^{a-1}$ divisé par $a$, laisse le reste 1; donc $x^{(a-1)m+n}$ divisé par $a$, laissera le même reste que $x^{n}$.

(347) Il suit du Théorême précédent, que l'équation $\frac{x^{n}-b}{a}=e$ aura toujours une solution, quel que soit $b$, lorsque $n$ et $a-1$ seront premiers entr'eux; soit alors $\pi$ le plus petit nombre positif qui satisfait à l'équation $\pi n-\rho(a-1)=1$, cette solution sera $x=b^{\pi}$.

En général, ce Théorême a l'avantage d'indiquer tout à-la-fois si l'équation proposée est résoluble, combien elle a de solutions, et quelle est l'équation la plus simple qui contient toutes ces solutions. Dans l'équation réduite, l'exposant de $x$ sera toujours diviseur de $a-1$; ainsi il ne s'agit plus que de trouver les solutions de l'équation $\frac{x^{n}-b}{a}=e$, dans la supposition que $n$ soit diviseur de $a-1$. Or il est facile de voir que si on connoît une des valeurs de $x$, on les aura toutes en multipliant la valeur connue par les différentes racines de l'équation $\frac{x^{n}-1}{a}=e$; il convient donc avant tout, de s'occuper de la résolution de cette dernière équation.

(348) THÉORÈME II. *Étant proposée l'équation* $\frac{x^n - 1}{a} = e$, *dans laquelle* a *est un nombre premier, et* n *un diviseur de* $a - 1$, *en sorte qu'on ait* $a - 1 = a'n$,

1°. *On aura* $x = u^{a'}$, u *étant un nombre quelconque non divisible par* a.

2°. *Si* $\theta$ *est une valeur de* x, $\theta^m$ *en sera une aussi, quel que soit l'exposant* m.

3°. *Si le nombre* $\theta$ *est tel que* $\theta^{\frac{n}{\nu}} - 1$ *ne soit pas divisible par* a, $\nu$ *étant un diviseur premier de* n, *la formule* $x = \theta^m$ *contiendra toutes les solutions de l'équation proposée, lesquelles seront* 1, $\theta$, $\theta^2 \ldots \theta^{n-1}$, *ou les restes de ces quantités divisées par* a.

4°. *Non-seulement il y a plusieurs nombres* $\theta$ *qui jouissent de cette propriété, mais le nombre en est* $n\left(1 - \frac{1}{\nu}\right)\left(1 - \frac{1}{\nu'}\right)\left(1 - \frac{1}{\nu''}\right)$&c., $\nu$, $\nu'$, $\nu''$, &c. *étant les différens nombres premiers qui peuvent diviser* n.

Car 1°. si l'on fait $x = u^{a'}$, on aura $x^n - 1 = u^{a'n} - 1 = u^{a-1} - 1$, quantité toujours divisible par $a$.

2°. Si $x = \theta$, on aura, en rejetant les multiples de $a$, $\theta^n = 1$ : faisant donc $x = \theta^m$, on aura pareillement $x^n = \theta^{mn} = 1$, quel que soit $m$.

3°. L'équation proposée devant avoir $n$ solutions, la formule $x = \theta^m$ les donnera toutes, si dans la suite 1, $\theta$, $\theta^2$, $\theta^3 \ldots \theta^{n-1}$, il n'y a pas deux termes égaux (en rejetant toujours les multiples de $a$). Or supposons $\theta^\mu = \theta^\lambda$, il en résultera $\theta^\sigma = 1$, $\sigma$ étant $\mu - \lambda$ ou $\lambda - \mu$, et par conséquent moindre que $n$. Mais comme on a déjà $\theta^n = 1$, si on appelle $\varepsilon$ le commun diviseur de $\sigma$ et de $n$, et qu'on résolve l'équation $ny - \sigma z = \varepsilon$, on aura $\theta^{ny} = \theta^{\sigma z + \varepsilon}$; le premier membre, à cause de $\theta^n = 1$, se réduit à 1 ; le second, à cause de $\theta^\sigma = 1$, se réduit à $\theta^\varepsilon$; ainsi on auroit $\theta^\varepsilon = 1$ ; soit $n = \varepsilon n'$, et $n' = n''\nu$, $\nu$ étant un nombre premier ; puisqu'on a $\theta^\varepsilon = 1$, on aura aussi $\theta^{\varepsilon n''} = 1$, ou $\theta^{\frac{n}{\nu}} = 1$, équation impossible, puisqu'on a supposé dans l'énoncé du Théorême, que la quantité $\theta^{\frac{n}{\nu}} - 1$ ne peut

être divisible par $a$; donc la formule $x=\theta^m$ renfermera implicitement toutes les solutions de l'équation proposée.

4°. Soit $\nu$ l'un des diviseurs premiers de $n$; de même qu'il n'y a que $n$ valeurs de $x$ qui satisfont à l'équation $\frac{x^n-1}{a}=e$, il n'y a aussi que $\frac{n}{\nu}$ valeurs de $\theta$ qui donnent $\theta^{\frac{n}{\nu}}=1$. Donc sur $n$ valeurs que doit avoir $\theta$ dans l'équation $\theta^n=1$, il y en a $n-\frac{n}{\nu}$ qui ne donnent pas $\theta^{\frac{n}{\nu}}=1$. Raisonnant de même à l'égard des autres facteurs premiers dont $n$ peut être composé, on conclura qu'il y a un nombre $n\left(1-\frac{1}{\nu}\right)\left(1-\frac{1}{\nu'}\right)\left(1-\frac{1}{\nu''}\right)$, &c. de valeurs de $\theta$, telles qu'aucune des quantités $\theta^{\frac{n}{\nu}}-1$, $\theta^{\frac{n}{\nu'}}-1$, $\theta^{\frac{n}{\nu''}}-1$, &c., n'est divisible par $a$.

(349) Donc si $n$ est un nombre premier, il suffira d'avoir une valeur de $x$ autre que l'unité, et cette valeur étant nommée $\theta$, la formule $x=\theta^m$ contiendra toutes les valeurs de $x$.

Si $n$ est une puissance d'un nombre premier $\nu$, pour que la valeur $x=\theta$ qui satisfait à l'équation $x^n=1$, en donne la solution complète, il faudra que $\theta^{\frac{n}{\nu}}$ ne soit pas égale à $+1$, et alors on aura $x=\theta^m$.

Enfin si $n$ est de la forme $\nu^\alpha\,\nu'^\mathcal{C}\,\nu''^\gamma$ &c. comme on peut toujours le supposer, je fais $\nu^\alpha=\mu$, $\nu'^\mathcal{C}=\mu'$, $\nu''^\gamma=\mu''$, &c., et je résous séparément les équations

$$\frac{x^\mu-1}{a}=e\,,\quad \frac{x^{\mu'}-1}{a}=e\,,\quad \frac{x^{\mu''}-1}{a}=e\,,\quad \text{\&c.}$$

Soient $x=\lambda^m$, $x=\lambda'^m$, $x=\lambda''^m$, &c. les solutions complètes de ces équations, je dis qu'en prenant $\theta=\lambda\lambda'\lambda''$ &c., la formule $x=\theta^m$ sera la solution complète de l'équation proposée. C'est un moyen qu'on pourra mettre en usage, lorsqu'on n'aura pas rencontré tout d'un coup, par la formule $x=u^{\alpha'}$, le nombre $\theta$ propre à donner toutes les solutions.

### EXEMPLE I.

(350) On demande les sept valeurs que doit avoir $x$ dans l'équation $\frac{x^7-1}{379}=e$?

Puisque $379-1=7.54$, on aura $x=u^{54}$, $u$ étant un nombre quelconque non divisible par 379. Soit $u=2$, on aura, en rejetant successivement les multiples de 379, $u^6=64$, $u^{12}=-73$, $u^{24}=23$, $u^{48}=150$, $u^{54}=125$. Donc $x=125$, et comme l'exposant 7 est un nombre premier, toutes les valeurs de $x$ seront comprises dans la formule $x=125^m$, laquelle donne les sept nombres suivans 1, 125, 86, 138, $-184$, 119, 94. La moindre valeur de $x$ étant 86, on voit qu'il auroit été fort long de chercher les valeurs de $x$ par le tâtonnement, en faisant successivement $x=\pm1$, $\pm2$, $\pm3$, &c.

### EXEMPLE II.

(351) Étant proposée l'équation $\frac{x^{63}-1}{379}=e$, on peut d'après le n°. 349 résoudre les équations $\frac{x^9-1}{379}=e$, $\frac{x^7-1}{379}=e$. Celles-ci ayant pour solutions complètes $x=180^m$, $x=125^m$, on en conclura celle de la proposée $x=(180.125)^m=139^m$; et comme le quarré de 139, divisé par 379, laisse le reste $-8$, on a plus simplement $x=(-8)^m$.

La même équation auroit donné immédiatement, par la première partie du Théorême II, $x=u^6$. Soit $u=2$, on aura $x=64$; et comme les diviseurs premiers de $n=63$ sont 3 et 7, il faut voir si $64^{21}$ et $64^9$ ne donneront pas pour reste $+1$. Or on trouve que ces puissances ne donnent pas le reste $+1$; donc $64^m$ eût été encore la solution complète de la même équation.

(352) THÉORÊME III. *Étant proposée l'équation* $\frac{x^{2n}+1}{a}=e$, *dans laquelle* a *est premier et* 4n *diviseur de* a$-1$, *on résoudra l'équation* $\frac{x^{4n}-1}{a}=e$ *qui sera toujours possible. Soit* $x=\theta^m$ *la*

*solution complète de celle-ci, je dis que la solution complète de la proposée sera* $x=\theta^{2i+1}$, *i étant un nombre quelconque.*

Car $\theta^m$ étant une valeur quelconque de $x$ dans l'équation $\frac{x^{4n}-1}{a}=e$, $\theta^{2m}$ sera aussi une valeur quelconque de $x$ dans l'équation $\frac{x^{2n}-1}{a}=e$. Restent donc les puissances impaires de $\theta$ pour résoudre l'équation $\frac{x^{2n}+1}{a}=e$.

### Exemple.

(353) Soit proposée l'équation $\frac{x^{36}+1}{433}=e$, qui est résoluble, parce que $433-1$ divisé par 36, donne le nombre pair 12.

Je me servirai pour cela de l'équation $\frac{x^{72}-1}{433}=e$, qui donne $x=u^6$. Soit $u=5$, on aura $u^6$ ou $x=37$. Cette valeur étant nommée $\theta$, on a $\theta^{36}=-1$, $\theta^{2i}=198$; donc suivant les parties 2ème et 3ème du Théorême II, $\theta^m$ est la solution complète de l'équation $\frac{x^{72}-1}{433}=e$, et par conséquent $\theta^{2i+1}$ est celle de la proposée $\frac{x^{36}+1}{433}=e$. Voici les trente-six solutions qui en résultent.

$$x=37^{2i+1}=\pm 37\pm 8\pm 127\pm 203\pm 79\pm 99\pm 2\pm 140\pm 159$$
$$\pm 128\pm 133\pm 216\pm 35\pm 148\pm 32\pm 75\pm 54\pm 117.$$

Les mêmes valeurs seroient renfermées plus simplement dans la formule $x=2^{2i+1}$.

(354) Théorème IV. *Étant proposée l'équation* $\frac{x^n-b}{a}=e$ *dans laquelle* $b^m=\pm 1$, m *étant diviseur de* $\frac{a-1}{n}$,

1°. *Si* m *et* n *sont premiers entr'eux, et qu'on cherche les nombres positifs* $\pi$ *et* $\varphi$ *tels que* $\pi n-\varphi m=1$, *je dis qu'on aura* $x=b^{\pi}y$, y *étant une racine quelconque de l'équation* $\frac{y^n-(\pm 1)^{\varphi}}{a}=e$;

2°. *Si* m *et* n *ont un commun diviseur* $\omega$; *soit* $n=n'\omega$

et.

et $\pi n' - \rho m = 1$, *on aura* $x^n = b^\pi y$, *ou* $\frac{x^n - b^\pi y}{a} = e$, $y$ *étant une racine quelconque de l'équation* $\frac{y^{n'} - (\pm 1)^\rho}{a} = e$.

Car en faisant dans le second cas $x^n = b^\pi y$, on a $x^{n'n}$ ou $x^n = b^{\pi n'} y^{n'} = b^{1+\rho m} (\pm 1)^\rho = b$. Le premier cas est d'ailleurs une suite dn second.

Ce Théorême offre déjà un grand nombre de cas où l'on peut rappeler immédiatement l'équation $\frac{x^n - b}{a} = e$ à la forme $\frac{x^n \pm 1}{a} = e$. Il indiqne en même temps une infinité d'antres cas où l'équation $\frac{x^n - b}{a} = e$ se décompose d'elle-même en un nombre $n'$ d'équations de degré inférieur $\frac{x^m - b^\pi y}{a} = e$.

EXEMPLE I.

(355) Soit l'équation $\frac{x^3 + 49}{223} = e$, qui est résoluble (Th. I), parce qu'on a $(-49)^{74} = 1$. Les nombres 3 et 74 étant premiers entr'eux, on aura, suivant le Théorême précédent, $x = (-49)^{25} y = -66y$, $y$ étant une racine de l'équation $\frac{y^3 - 1}{223} = e$.

*Remarquez* que si on eût proposé l'équation $\frac{x^3 + 7}{223} = e$, il eût été facile de voir qu'une de ses racines est $x = 6$. Or il suit de-là que dans l'équation $\frac{x^3 + 49}{223} = e$, on a $x = -36$. En effet, les trois racines de cette dernière sont $x = -36$, $-66$, $102$.

En général, si $\alpha$ est une solution de l'équation $\frac{x^n - b}{a} = e$, $\alpha^k$ en sera une de l'équation $\frac{x^n - b^k}{a} = e$.

EXEMPLE II.

(356) Etant proposée l'équation $\frac{x^6 + 20}{61} = e$, où l'on a $b = -20$, il faut d'abord, pour que cette équation soit possible (n°. 346),

qu'on ait, en négligeant les multiples de 61, $b^{10}=1$. Or on trouve $b^5=-1$, et par conséquent $b^{10}=1$; donc l'équation est possible. Ensuite, puisque les exposans 6 et 5 sont premiers entr'eux, on aura, suivant le théorème, $x=-20y$, et $\frac{y^6+1}{61}=e$. Or l'équation $\frac{y^{12}-1}{61}=e$ a pour solution complète $y=29^k$; donc $x=-20.29^{6i+1}=30.13^i$. Les nombres qui en résultent sont $\pm 7 \pm 24 \pm 30$.

### Exemple III.

(357) Soit l'équation $\frac{x^{10}-5}{601}=e$, on trouve $b^6=-1$; mais comme 10 et 6 ont pour commun diviseur 2, on fera, suivant la seconde partie du théorème, $x^2=b^5y$ et $\frac{y^5-1}{601}=e$. Celle-ci donne $y=(-169)^k$; ainsi l'équation proposée peut se décomposer en cinq autres du second degré, qui sont :

$$\frac{x^2-120}{61}=e,\ \frac{x^2-154}{601}=e,\ \frac{x^2+183}{601}=e,\ \frac{x^2-276}{601}=e,\ \frac{x^2-234}{601}=e.$$

Mais cette décomposition est peu avantageuse, car il suffit d'avoir une valeur de $x$ qu'on multipliera par les racines de l'équation $\frac{y^{10}-1}{601}=e$; on peut donc n'employer qu'une de ces équations, et la troisième, qui est la même que $\frac{x^3+28^3}{601}=e$, est celle d'où l'on tirera le plus aisément une valeur de $x$ (n°. 286).

(358) Théorème V. *Soit l'équation à résoudre* $\frac{x^n-b}{a}=e$ *dans laquelle* $b^\omega=1$, $\omega$ *étant diviseur de* $\frac{a-1}{n}$; *soit* $x=\theta^m$ *la solution complète de l'équation* $\frac{x^{n\omega}-1}{a}=e$; $b$ *devant être un des nombres* $\theta^n, \theta^{2n}, \theta^{3n} \ldots \theta^{(\omega-1)n}$, *je suppose* $b=\theta^{\mu n}$ : *cela posé, je dis que la solution complète de l'équation proposée sera* $x=\theta^{m\omega+\mu}$.

En effet cette valeur de $x$ donne $x^n=b$, quelle que soit $m$; il suffit

donc de faire voir que $b$ se trouvera toujours parmi les nombres $\theta^{n}$, $\theta^{2n}$, &c. Or puisque $\theta^{m}$ est la solution complète de l'équation $\frac{x^{n\omega}-1}{a}=e$, on aura $\theta^{mn}$ pour celle de l'équation $\frac{x^{\omega}-1}{a}=e$, et puisque $b^{\omega}=1$, il est clair que $b$ doit être un des nombres représentés par $\theta^{mn}$.

Cette méthode pour résoudre l'équation $\frac{x^{\omega}-b}{a}=e$, n'est sujette à aucune exception; mais il peut être plus ou moins long de chercher $b$ dans la suite $\theta^{n}$, $\theta^{2n}$, &c., et pour qu'elle réussisse complettement, il faut que le nombre $\omega$ ne soit pas bien grand. Si l'équation $b^{\omega}=1$ résultoit de l'équation $b^{\frac{1}{2}\omega}=-1$, il ne faudroit chercher $b$ que dans la suite $\theta^{n}$, $\theta^{3n}$, $\theta^{5n}$, &c.

EXEMPLE.

(359) Soit l'équation $\frac{x^{12}-5}{601}=e$, déjà traitée (357), mais qui n'a pu se décomposer qu'en facteurs du second degré. On aura, en rejetant les multiples de 601, $b=5$, $b^{6}=-1$, $b^{12}=1$, et ainsi $\omega=12$. Maintenant la solution complète de l'équation $\frac{x^{600}-1}{601}=e$, trouvée par le Théorême II, est $x=(-140)^{m}$; et par conséquent celle de l'équation $\frac{x^{12}-1}{601}=e$ est $x=(-140)^{50\mu}$ ou $120^{\mu}$; donc $b$ doit être compris dans la formule $120^{\mu}$, en prenant pour $\mu$ un nombre impair : or on trouve qu'il faut pour cela faire $\mu=5$. Donc la solution complète de l'équation proposée sera $x=(-140)^{?+50m}$ ou $x=214.(169)^{m}$. Les valeurs qui en résultent sont $\pm 214$, $\pm 106$, $\pm 116$, $\pm 229$, $\pm 237$.

(360) Ayant trouvé un nombre $\theta$ tel que $\theta^{n}-b$ est divisible par le nombre premier $a$, il est facile de trouver une valeur de $x$ telle que $x^{n}-b$ soit divisible par une puissance quelconque $a^{\kappa}$ de ce nombre premier. Pour cela, soit $\theta^{n}-b=Ma$, si l'on fait 1°. $x=\theta+Aa$, et qu'on détermine $A$ et $M'$ par l'équation $M+n\theta^{n-1}A=aM'$, il est clair que $x^{n}-b$ sera divisible par $a^{2}$.

Si on fait 2°. $\theta' = \theta + \mathcal{A}\,a$, $x = \theta' + \mathcal{A}'a^2$, et qu'on détermine $\mathcal{A}'$ et $M''$ par l'équation $M' + n\theta'^{n-1}\mathcal{A}' = a^2 M''$, la quantité $x^n - b$ sera divisible par $a^4$.

Si on fait 3°. $\theta'' = \theta' + \mathcal{A}'a^2$, $x = \theta'' + \mathcal{A}''a^4$, et qu'on détermine $\mathcal{A}''$ et $M'''$ par l'équation $M'' + n\theta''^{n-1}\mathcal{A}'' = a^4 M'''$, le binome $x^n - b$ sera divisible par $a^8$.

On continuera ainsi jusqu'à ce que $x^n - b$ soit divisible par $a^\alpha$; et si $\alpha$ n'étoit pas un terme de la suite 2, 4, 8, 16, &c., on voit aisément quel changement il faudroit apporter à la dernière des équations indéterminées. Ainsi si on avoit $\alpha = 7$, au lieu de la troisième équation $M'' + n\theta''^{n-1}\mathcal{A}'' = a^4 M'''$, on prendroit $M'' + n\theta''^{n-1}\mathcal{A}'' = a^3 M''$, et la valeur $x = \theta'' + \mathcal{A}''a^4$ rendroit $x^n - b$ divisible par $a^7$.

*Nota.* Si l'exposant $n$ étoit divisible par $a$, il pourroit arriver que quelqu'une des équations qui servent à déterminer $\mathcal{A}$, $\mathcal{A}'$, $\mathcal{A}''$, &c., fût impossible; mais alors on auroit acquis la preuve que $x^n - b$ ne peut être divisible par $a^\alpha$.

(361) Maintenant si l'on veut que $x^n - B$ soit divisible par un nombre composé quelconque $\mathcal{A} = a^\alpha b^\zeta c^\gamma$, &c. dont $a^\alpha$, $b^\zeta$, $c^\gamma$, &c. sont les facteurs premiers, élevés à des puissances quelconques; il faudra, par ce qui précède, déterminer les nombres $\lambda$, $\mu$, $\nu$, &c., tels que les quantités

$$\frac{\lambda^n - B}{a^\alpha}, \quad \frac{\mu^n - B}{b^\zeta}, \quad \frac{\nu^n - B}{c^\gamma}, \quad \&c.$$

soient des entiers. Ensuite on combinera ensemble les équations

$$x = \lambda + a^\alpha z = \mu + b^\zeta z' = \nu + c^\gamma z'' = \&c.$$

Et on obtiendra de cette manière toutes les valeurs de $x$, moindres que $\frac{1}{2}\mathcal{A}$, qui rendent $x^n - B$ divisible par $\mathcal{A}$, ou qui satisfont en général à l'équation $x^n - B = \mathcal{A}y$.

Si on avoit à résoudre l'équation $Cx^n - B = \mathcal{A}y$, on pourra supposer que $C$ et $\mathcal{A}$ n'ont point de commun diviseur; (car s'ils en avoient un, on le feroit disparoître par la division). Soit donc $C\mu - \mathcal{A}\nu = 1$, si l'on fait $y' = \mu y - \nu x^n$, l'équation à résoudre deviendra $x^n - B\mu = \mathcal{A}y'$, et ainsi sera ramenée au cas déjà traité.

## §. III. *Méthode pour trouver le diviseur quadratique qui renferme le produit de plusieurs diviseurs quadratiques donnés.*

(362) Problème I. *Étant donnés deux diviseurs quadratiques* $\Delta$, $\Delta'$, *d'une même formule* $t^2+au^2$, *trouver le diviseur quadratique qui renferme leur produit* $\Delta\Delta'$.

Nous distinguerons deux cas, selon que les diviseurs proposés sont de la forme ordinaire $py^2+2qyz+rz^2$ ou de la forme $py^2+qyz+rz^2$ dont les coefficiens sont impairs.

*Premier Cas.* Soit $\Delta=py^2+2qyz+rz^2$ et $\Delta'=p'y'^2+2q'y'z'+r'z'^2$, nous supposerons que les coefficiens $p$ et $p'$ sont premiers entre eux, ou que du moins ils ont été rendus tels par une préparation convenable. Cela posé, si l'on fait $py+qz=x$, $p'y'+q'z'=x'$, on aura $p\Delta=x^2+az^2$, $p'\Delta'=x'^2+az'^2$, donc

$$pp'\Delta\Delta'=(xx'\pm azz')^2+a(xz'\mp x'z)^2.$$

Mais puisqu'on veut que le produit $\Delta\Delta'$ soit contenu dans un diviseur quadratique de la formule $t^2+au^2$; puisque d'ailleurs ce produit, considéré en général, doit contenir le produit particulier $pp'$, on pourra supposer $\Delta\Delta'=pp'Y^2+2\varphi YZ+\psi Z^2$ et $pp'\psi-\varphi^2=a$, ce qui donnera

$$pp'\Delta\Delta'=(pp'Y+\varphi Z)^2+aZ^2.$$

Comparant cette valeur à la précédente, on aura

$$pp'Y+\varphi Z=xx'\pm azz'$$
$$Z=xz'\mp x'z.$$

Mettant au lieu de $a$ sa valeur $pp'\psi-\varphi^2$, la première de ces deux équations donnera

$$pp'Y=(x\pm\varphi z)(x'-\varphi z')\pm pp'\psi zz';$$

et en substituant de nouveau à la place de $x$ et $x'$ leurs valeurs $py+qz$ et $p'y'+q'z'$, on aura, après avoir divisé par $pp'$,

$$Y=\left(y+\frac{q\pm\varphi}{p}z\right)\left(y'+\frac{q'-\varphi}{p'}z'\right)\pm\psi zz'.$$

Cette quantité doit être un nombre entier, indépendamment de toutes valeurs de $z$ et de $z'$, il faut donc que $\frac{q\pm\varphi}{p}$ et $\frac{q'-\varphi}{p'}$ soient des entiers. Soit en conséquence

$$\varphi = pn \mp q = p'n' + q' ; \qquad \text{(a)}$$

on pourra toujours déterminer $n$ et $n'$ par l'équation $pn\mp q=p'n'+q'$, puisque $p$ et $p'$ sont premiers entr'eux ; on aura ainsi la valeur de $\varphi$, laquelle donnera un nombre entier pour $\psi=\frac{\varphi^2+a}{pp'}$. Car ayant $\varphi=pn\mp q$, et $q^2+a=pr$, il s'ensuit que $\varphi^2+a$ est divisible par $p$ ; ayant de même $\varphi=p'n'+q'$ et $q'^2+a=p'r'$, il s'ensuit que $\varphi^2+a$ est divisible par $p'$ ; donc puisque $p$ et $p'$ sont premiers entre eux, il faudra que $\varphi^2+a$ soit divisible par $pp'$.

Les nombres $n$, $n'$, $\varphi$, $\psi$ étant déterminés comme on vient de le dire, si l'on fait

$$Y=(y\pm nz)(y-n'z')\pm\psi zz'$$
$$Z=xz'\mp x'z=(py+qz)z'\mp(p'y'+q'z')z,$$

on aura le produit cherché

$$\Delta\Delta'=pp'Y^2+2\varphi YZ+\psi Z^2;$$

de sorte que ce produit sera contenu dans un nouveau diviseur quadratique de la même formule $t^2+au^2$.

(363) On doit remarquer, à cause de l'ambiguité du signe $\pm$ dans l'équation (a), que le problême considéré en général a deux solutions. Mais il ne peut en avoir plus de deux. En effet, on peut supposer les nombres $p$ et $p'$ premiers l'un et l'autre ; et le diviseur quadratique, quel qu'il soit, qui renferme $\Delta\Delta'$, sera toujours de la forme $pp'y^2+2\varphi yz+\psi z^2$, où l'on a $\varphi^2+a=pp'\psi$. Mais lorsque les nombres $p$ et $p'$ sont premiers, il n'y a que deux valeurs de $\varphi$, moindres que $\frac{1}{2}pp'$, qui rendent $\varphi^2+a$ divisible par $pp'$. Donc il n'y a au plus que deux diviseurs quadratiques différens qui renferment le produit $\Delta\Delta'$. Je dis *au plus*, parce que dans quelques cas particuliers les deux diviseurs quadratiques réduits à l'expression la plus simple, pourront coincider en un seul, lequel contiendroit $\Delta\Delta'$ dans deux combinaisons différentes. Cela doit arriver, ainsi qu'on en verra un exemple, lorsque la formule $t^2+au^2$ ne

contient qu'un seul diviseur quadratique correspondant aux formes linéaires dans lesquelles $pp'$ est compris.

(364) *Second Cas.* Si le nombre $a$ est de forme $8n+3$, et qu'en conséquence le diviseur quadratique $\Delta$, qu'on supposera impair, soit de la forme $py^2+qyz+rz^2$, dans laquelle les coefficiens $p, q, r$ sont impairs, et où l'on a $4pr-q^2=a$, on pourra encore faire usage de l'analyse précédente, pour avoir le produit $\Delta\Delta'$. En effet comme on a $2\Delta=2py^2+2qyz+2rz^2$, $2\Delta'=2p'y'^2+2q'y'z'+2r'z'^2$, il suffira de mettre dans les formules trouvées $2p$ et $2r$ à la place de $p$ et $r$. On aura donc, pour déterminer $n$ et $n'$, l'équation

$$pn-p'n'=\tfrac{1}{2}(q'\pm q); \qquad \text{(b)}$$

d'où on déduira les valeurs de $\varphi$ et $\psi$, savoir $\varphi=2pn\mp q$, $\psi=\dfrac{\varphi^2+a}{pp'}$. Faisant ensuite $Y=(y\pm nz)\,(y-n'z')\pm\psi zz'$, $Z=(2py+qz)z'\mp(2p'y'+q'z')z$, on aura

$$4\Delta\Delta'=4pp'Y^2+2\varphi YZ+\psi Z^2.$$

Or on voit que $Z$ étant toujours pair, on peut mettre $2Z$ à la place de $Z$, et alors si l'on fait de nouveau

$$Y=(y\pm nz)\,(y-n'z')\pm\psi zz'$$
$$Z=pyz'\mp p'y'z+\tfrac{1}{2}(q\mp q')zz',$$

le produit cherché sera

$$\Delta\Delta'=pp'Y^2+\varphi YZ+\psi Z^2.$$

### EXEMPLE I.

(365) Soient proposées les deux formules $\Delta=14y^2+10yz+21z^2$, $\Delta'=9y'^2+2y'z'+30z'^2$, lesquelles représentent deux diviseurs quadratiques de la formule $t^2+269u^2$. Pour avoir le produit $\Delta\Delta'$ exprimé par une formule de même nature, j'observe que les coefficiens 14 et 9 étant premiers entr'eux, on peut, sans aucune préparation, appliquer à cet exemple les formules du n°. 362. Faisant donc $p=14$, $q=5$, $p'=9$, $q'=1$, on aura l'équation $14n\mp5=9n'+1$, laquelle donne deux résultats différens, selon qu'on prend le signe supérieur ou l'inférieur.

1°. Avec le signe supérieur on aura $n=3$, $n'=4$, $\varphi=37$, $\psi=13$, de sorte qu'en faisant

$$Y = yy' + 3zy' - 4yz' + zz'$$
$$Z = 14yz' - 9y'z + 4zz',$$

le produit cherché sera

$$\Delta\Delta' = 126\,Y^2 + 74\,YZ + 13\,Z^2.$$

2°. Avec l'autre signe, on trouve $n=1$, $n'=2$, $\varphi=19$, $\psi=5$; donc en faisant

$$Y = yy' - zy' - 2yz' - 3zz'$$
$$Z = 14yz' + 9zy' + 6zz',$$

le même produit sera de nouveau

$$\Delta\Delta' = 126\,Y^2 + 38\,YZ + 5\,Z^2.$$

Maintenant, pour réduire ces produits à l'expression la plus simple, il faut faire dans le premier cas $Z = U - 2Y$, et dans le second $Z = U - 4Y$, ce qui donnera finalement ces deux résultats :

$$(1)\begin{cases} U = 2yy' + 6yz' - 3yz' + 6zz' \\ Y = yy' + 3y'z - 4yz' + zz' \\ \Delta\Delta' = 13\,U^2 + 22\,UY + 30\,Y^2. \end{cases}$$

$$(2)\begin{cases} U = 4yy' + 5y'z + 6yz' - 6zz' \\ Y = yy' - y'z - 2yz' - 3zz' \\ \Delta\Delta' = 5\,U^2 - 2\,UY + 54\,Y^2. \end{cases}$$

### EXEMPLE II.

(366) Soient proposés les diviseurs $\Delta = y^2 + yz + 41z^2$, $\Delta' = y'^2 + y'z' + 41z'^2$, tous deux appartenans à la formule $t^2 + 163u^2$. Pour avoir leur produit exprimé d'une manière semblable, on suivra les formules du n°. 364, lesquelles donneront les deux résultats que voici :

$$(1)\begin{cases} Y = yy' + zy' + 41zz' \\ Z = yz' - y'z \\ \Delta\Delta' = Y^2 + YZ + 41\,Z^2. \end{cases}$$

$$(2)\begin{cases} Y = yy' - 41zz' \\ Z = yz' + y'z + zz' \\ \Delta\Delta' = Y^2 + YZ + 41\,Z^2. \end{cases}$$

Dans

Dans les deux cas, le produit est de même forme que les deux facteurs; et en effet il ne peut être de forme différente, puisque la formule $t^2+163u^2$ n'est susceptible que d'un seul diviseur quadratique.

(367) Problème II. *Trouver le produit de deux diviseurs quadratiques semblables* $\Delta = py^2+2qyz+rz^2$, $\Delta' = py'^2+2qy'z'+rz'^2$.

On pourroit, par une transformation, réduire ce problème au précédent; mais il est plus simple de procéder à la résolution directe de la manière suivante :

Soit $py+qz=x$, $py'+qz'=x'$, on aura

$$\Delta\Delta' p^2 = (x^2+az^2)(x'^2+az'^2) = (xx' \pm azz')^2 + a(xz' \mp x'z)^2.$$

Si dans les signes ambigus du second membre on prend le signe inférieur, et qu'on remette les valeurs de $x$ et $x'$ ainsi que celle de $a$, on aura $xx'+azz' = p^2yy'+pq(yz'+y'z)+przz'$, et $xz'-x'z = p(yz'-y'z)$; d'où l'on tire, après avoir divisé par $p^2$,

$$\Delta\Delta' = (pyy'+qyz'+qy'z+rzz')^2 + a(yz'-y'z)^2.$$

C'est la première valeur du produit $\Delta\Delta'$, laquelle est de la forme $y^2+az^2$.

Pour avoir une seconde valeur de ce produit, supposons $\Delta\Delta' = p^2Y^2+2\varphi YZ+\psi Z^2$, et à l'ordinaire $p^2\psi-\varphi^2=a$; nous aurons $\Delta\Delta' p^2 = (p^2Y+\varphi Z)^2+aZ^2$; de sorte qu'en comparant cette valeur à la première, on aura

$$Z = xz' \mp x'z$$
$$p^2Y+\varphi Z = xx' \pm azz',$$

substituant dans la dernière équation la valeur de $a$, ainsi que celles de $x$, $x'$, et $Z$, on en tire

$$Y = \left(y+\frac{q\pm\varphi}{p}z\right)\left(y'+\frac{q-\varphi}{p}z'\right) \pm \psi zz'.$$

Donc pour que $Y$ soit entier, indépendamment de toute valeur particulière de $z$ et $z'$, il faut que $\frac{q\pm\varphi}{p}$ et $\frac{q-\varphi}{p}$ soient des entiers; de-là on voit que dans les signes ambigus on doit prendre seulement le signe inférieur; c'est pourquoi faisant $\varphi = q+pn$, on aura

$$Y = (y-nz)(y'-nz') - \psi zz'$$
$$Z = p(yz'+y'z)+2qzz'.$$

Mais il reste à déterminer $n$ de manière que $\psi$ soit un entier : or on a $\psi = \frac{a+\varphi^2}{p^2} = \frac{pr-q^2+(q+pn)^2}{p^2} = \frac{r+2qn}{p} + n^2$. Donc si l'on cherche les plus petites valeurs de $m$ et $n$ qui satisfont à l'équation

$$r = pm - 2qn,$$

toutes les conditions seront remplies ; on aura $\varphi = q + pn$, $\psi = m + n^2$, et le produit demandé sera dans sa seconde forme,

$$\Delta\Delta' = p^2Y^2 + 2\varphi YZ + \psi Z^2.$$

(368) L'équation $r = pm - 2qn$ dans laquelle $m$ et $n$ sont des indéterminées, sera toujours résoluble tant que $p$ et $2q$ seront premiers entr'eux ; elle le seroit encore, si $p$ et $2q$ ayant un commun diviseur $\theta$, $r$ étoit aussi divisible par $\theta$. Ce cas cependant importe peu à considérer, ou même doit être entièrement écarté, parce qu'alors la formule $py^2+2qyz+rz^2$ ne pourroit représenter que des nombres divisibles par $\theta$.

Enfin il peut arriver que $p$ et $q$ aient un commun diviseur $\theta$, lequel ne soit pas commun avec $r$, alors l'équation $r = pm - 2qn$ seroit impossible. C'est ce qui aura lieu dans les deux cas ci-après.

1°. Si $a$ est divisible par $\theta$ et non par $\theta^2$, car alors $p$ divise bien $t^2+au^2$, mais $p^2$ ne peut diviser cette formule qu'en supposant que $t$ et $u$ ne sont pas premiers entr'eux.

2°. Si $\theta$ étant diviseur commun de $p$ et $q$, les nombres $p$ et $a$ sont divisibles par $\theta^2$ ; car alors l'équation $pr - q^2 = a$ pourroit avoir lieu, sans que $r$ fût divisible par $\theta$. Dans ce cas, une simple transformation du diviseur $py^2+2qyz+rz^2$ préviendroit la difficulté ; ou bien, comme ce diviseur est alors de la forme $p'\theta^2y^2+2q'\theta yz+rz^2$, tandis que la formule qu'il divise est $t^2+a'\theta^2u^2$, on peut mettre $y$ à la place de $\theta y$, et $u$ à la place de $\theta u$, et on aura $p'y^2+2q'yz+rz^2$ pour diviseur de $t^2+a'u^2$. Or dans cette dernière forme, il n'y a plus lieu à difficulté.

(369) Si le nombre $a$ est de forme $8n+3$, et qu'en conséquence les diviseurs quadratiques proposés soient $\Delta = py^2+qyz+rz^2$ $\Delta' = py'^2+qy'z'+rz'^2$, on trouvera par une analyse semblable à

la précédente, deux formes du produit $\Delta\Delta'$. La première qui se présente immédiatement est

$$\Delta\Delta' = Y^2 + YZ + \tfrac{1}{4}(a+1)Z^2,$$

où l'on aura

$$Y = pyy' + \tfrac{1}{2}(q-1)yz' + \tfrac{1}{2}(q+1)y'z + rzz'$$
$$Z = yz' - y'z.$$

Pour avoir la seconde forme, il faut chercher les moindres valeurs de $m$ et $n$ qui satisfont à l'équation

$$r = pm - qn.$$

Faisant ensuite les constantes $\varphi = q + 2pn$, $\psi = m + n^2$, et les indéterminées

$$Y = (y - nz)(y' - nz') - \psi zz'$$
$$Z = p(yz' + y'z) + qzz';$$

on aura

$$\Delta\Delta' = p^2Y^2 + \varphi YZ + \psi Z^2.$$

(370) Il est manifeste que le problême général qu'on vient de résoudre comprend, comme cas particulier, celui où il s'agit de trouver le quarré d'un diviseur quadratique donné. Mais alors le produit n'est susceptible que d'une seule forme; car ayant $yz' - y'z = 0$, la première valeur de $\Delta\Delta'$ n'est pas de la forme d'un diviseur quadratique.

En général, puisqu'on peut exprimer le produit de deux diviseurs quadratiques donnés, égaux ou inégaux, par une formule de la même espèce, laquelle est aussi un diviseur quadratique, il s'ensuit qu'on pourra toujours trouver un diviseur quadratique égal au produit de plusieurs diviseurs quadratiques donnés.

Et si on s'occupe seulement de la forme des produits, sans s'inquiéter de la valeur des indéterminées qui y sont contenues, le problême devient beaucoup plus simple, puisqu'il suffit d'opérer sur les coefficiens, lesquels n'offrent qu'un nombre de combinaisons limité.

Ayant donc désigné, par exemple, par $A$, $B$, $C$, $D$, &c., les différens diviseurs quadratiques qui conviennent à une formule donnée $t^2 + au^2$, on cherchera, par les principes précédens, quelles doivent être les formes des différens produits deux à deux $AA$,

$AB$, $AC$, $BD$, &c. Si l'on trouve que le produit $AB$ peut être à-la-fois de la forme $C$ et de la forme $D$, on écrira $AB = \begin{cases} C \\ D \end{cases}$, et ainsi des autres. Or on conçoit que les produits deux à denx étant trouvés, on en déduira aisément les produits trois à trois, quatre à quatre, &c.; de sorte qu'on connoîtra en général les diverses formes du produit qui résulte de tant de diviseurs quadratiques qu'on voudra.

Dans cette notation, il convient de distinguer $BB$ de $B^2$; l'expression $BB$ désigne le produit de deux diviseurs quadratiques semblables à $B$, mais dont les indéterminées sont différentes; l'expression $B^2$ désigne le quarré du diviseur $B$, et suppose par conséquent que les deux facteurs $B$ et $B$ sont identiques, tant dans les coefficiens que dans les indéterminées; cette circonstance apporte une modification au résultat, car nous venons de voir que $B^2$ n'est susceptible que d'une forme, tandis que $BB$ en a toujours deux. Une pareille différence se fera sentir dans les expressions $BBB$, $B^2B$, $B^3$, et autres semblables : il est donc nécessaire de chercher à quelle forme doit répondre une puissance quelconque d'un diviseur quadratique donné. C'est l'objet du problême suivant.

(371) PROBLÊME III. *Étant donné un diviseur quadratique* $\Delta$ *de la formule* $t^2 + au^2$, *trouver le diviseur quadratique de la même formule, par lequel la puissance* $\Delta^n$ *puisse être exprimée.*

*Premier Cas.* Soit le diviseur donné $\Delta = py^2 + 2qyz + rz^2$, et supposons, pour éviter toute difficulté, que ce diviseur a été préparé de manière que le coefficient $p$ est un nombre premier non diviseur de $a$.

On peut d'abord démontrer qu'il n'existe qu'un seul diviseur quadratique dans lequel $\Delta^n$ puisse être contenu. En effet, quel que soit le diviseur quadratique qui contient $\Delta^n$, il devra contenir $p^n$. Or on a déjà prouvé (n°. 232) que $p$ étant un nombre premier, la puissance $p^n$ ne peut appartenir qu'à un seul diviseur quadratique. Donc il n'y a aussi qu'un seul diviseur quadratique qui puisse contenir $\Delta^n$.

Cela posé, puisqu'on a $pr = q^2 + a$, si l'on fait en général

$(q+\sqrt{-a})^n = F+G\sqrt{-a}$, $(q-\sqrt{-a})^n = F-G\sqrt{-a}$, on aura $(q^2+a)^n$ ou $p^n r^n = F^2 + a\,G^2$. Or je dis que $G$ et $p$ sont premiers entr'eux, car si $G$ étoit divisible par $p$, $F$ le seroit aussi d'après la dernière équation. Mais on a $F = q^n - \frac{n.n-1}{1.2} q^{n-2}\,a + \frac{n.n-1.n-2.n-3}{1.2.3.4} . q^{n-4}a^2 -$ &c., et si on néglige les multiples de $p$, on aura $a = -q^2$, et $F = q^n\left(1 + \frac{n.n-1}{1.2} + \frac{n.n-1.n-2.n-3}{1.2.3.4} + \&c.\right) = 2^{n-1}q^n$. Donc $q$, et par conséquent $a$, seroit divisible par $p$, ce qui est contre la supposition.

Puis donc que $G$ et $p$ sont premiers entr'eux, on pourra faire $F = \varphi\, G + p^n H$, $\varphi$ et $H$ étant des indéterminées, et en substituant cette valeur dans l'équation $p^n r^n = F^2 + a\,G^2$, on en conclura que $\varphi^2 + a$ est divisible par $p^n$, et qu'ainsi on peut faire $\varphi^2 + a = p^n\psi$.

Ayant déterminé de cette manière les quantités $\varphi$ et $\psi$, on aura le diviseur quadratique $p^n Y^2 + 2\,\varphi\, YZ + \psi\, Z^2$, lequel appartient à la formule $t^2 + a u^2$, puisqu'on a $p^n\psi - \varphi^2 = a$. Ce diviseur est celui qui contient généralement la puissance $\Delta^n$, puisqu'il contient le nombre $p^n$; mais il faut voir comment on déterminera $X$ et $Z$ en fonctions de $y$ et $z$.

Soit donc $\Delta^n = p^n Y^2 + 2\varphi YZ + \psi Z^2$, ou $\Delta^n p^n = (p^n Y + \varphi Z)^2 + aZ^2$: on a d'ailleurs $\Delta\, p = (py + qz)^2 + a\,z^2$; donc si l'on fait $py + qz = x$, $p^n Y + \varphi\, Z = X$, on aura $X^2 + a\,Z^2 = (x^2 + a\,z^2)^n$. Or on satisfait généralement à cette équation, en prenant $X + Z\sqrt{-a} = (x + z\sqrt{-a})^n$, d'où l'on tire

$$X = x^n - \frac{n.n-1}{1.2} x^{n-2} a z^2 + \frac{n.n-1.n-2.n-3}{1.2.3.4} x^{n-4} a^2 z^4 - \&c.$$

$$Z = nx^{n-1}z - \frac{n.n-1.n-2}{1.2.3} x^{n-3} a z^3 + \frac{n.n-1.n-2.n-3.n-4}{1.2.3.4.5} x^{n-5} a^2 z^5 - \&c.$$

La valeur de $Z$ est déjà exprimée par une fonction entière de $x$ et de $z$, ou par une de $y$ et de $z$; quant à $Y$, on a $Y = \frac{X - \varphi Z}{p^n}$: or $X^2 - \varphi^2 Z^2 = X^2 + aZ^2 - p^n\psi Z^2 = p^n(\Delta^n - \psi Z^2)$, donc il faut que $X^2 - \varphi^2 Z^2$ soit divisible par $p^n$. Mais on voit par l'équation $p^n\psi - \varphi^2 = a$ que $\varphi$ ne peut être divisible par $p$, puisqu'alors $a$ seroit divisible

aussi par $p$, contre la supposition. On ne peut supposer non plus que $Z$ soit divisible indéfiniment par $p$, car alors $X$ seroit aussi divisible par $p$, ainsi que $x^2+az^2$; donc en omettant les multiples de $p$, on auroit $az^2=-x^2$, valeur qui étant substituée dans celle de $X$, donne

$$X=x^n\left(1+\frac{n.n-1}{1.2}+\frac{n.n-1.n-2.n-3}{1.2.3.4}+\text{\&c.}\right)=2^{n-1}x^n;$$

donc il faudroit que $p$ divisât $x$, et par suite $z$, ce qui ne peut avoir lieu, puisque $y$ et $z$ sont des indéterminées à volonté.

Puisque la quantité $X^2-\varphi^2Z^2$ est divisible par $p^n$, et que ses deux facteurs $X+\varphi Z$, $X-\varphi Z$ ne peuvent avoir $p$ pour commun diviseur, il s'ensuit que l'un de ces facteurs est divisible par $p^n$. Et comme le signe de $\varphi$ est arbitraire, on pourra supposer que $X-\varphi Z$ représente celui des deux facteurs qui est divisible par $p^n$. Donc la valeur de $Y$ développée en fonction de $y$ et $z$, sera un nombre entier, quels que soient $y$ et $z$. Donc le diviseur quadratique $p^nY^2+2\varphi YZ+\psi Z^2$ ainsi déterminé, sera égal à la puissance $n$ du diviseur proposé $py^2+2qyz+rz^2$.

(372) *Second Cas.* Soit la formule donnée $\Delta=py^2+qyz+rz^2$, où l'on suppose $p$, $q$, $r$ impairs et $4pr-q^2=a$.

On préparera encore, s'il est nécessaire, cette formule de manière que le coefficient $p$ soit un nombre premier, et on démontreroit d'ailleurs, comme ci-dessus, qu'il n'y a qu'un seul diviseur quadratique qui puisse contenir la puissance demandée $\Delta^n$.

Représentons ce diviseur par la formule $p^nY^2+\varphi YZ+\psi Z^2$, il faudra qu'on ait $4p^n\psi=\varphi^2+a$. Or comme on a déjà $4pr=q^2+a$, si l'on fait $(\frac{1}{2}q+\frac{1}{2}\sqrt{-a})^n=\frac{1}{2}F+\frac{1}{2}G\sqrt{-a}$, les nombres $F$ et $G$ seront toujours entiers (n°. 57), parce que $a$ étant de la forme $8n+3$, $-a$ est de la forme $4n+1$ : on aura en même temps $(\frac{1}{2}q-\frac{1}{2}\sqrt{-a})^n=\frac{1}{2}F-\frac{1}{2}G\sqrt{-a}$, et par conséquent $\left(\frac{q^2+a}{4}\right)^n$ ou $p^nr^n=\frac{1}{4}(F^2+aG^2)$. Or on prouveroit, comme ci-dessus, que $F$ et $G$ sont premiers entr'eux, ou qu'ils ont seulement 2 pour commun diviseur ; donc on pourra faire $F=\varphi G+2p^nH$, c'est-à-dire qu'on pourra toujours déterminer le nombre impair $\varphi<p^n$

tel que $\frac{F-\phi G}{p^n}$ soit un entier. Cette valeur de $F$ étant substituée dans l'équation $4p^n r^n = F^2 + a G^2$, on en conclura que $\frac{\phi^2+a}{p^n}$ doit être un entier; et comme $\phi^2+a$ est de la forme $8n+4$, on aura en même temps $\frac{\phi^2+a}{4p^n}$ égal à un entier. Soit donc $\phi^2+a=4p^n\psi$, et il est clair que par le moyen de $\phi$ et $\psi$, on aura entièrement déterminé le diviseur quadratique qui contient $p^n$, lequel sera $p^nY^2+\phi YZ+\psi Z^2$.

Maintenant, je dis que ce diviseur contient en général $\Delta^n$, en sorte qu'on peut supposer $p^nY^2+\phi YZ+\psi Z^2 = \Delta^n = (py^2+qyz+rz^2)^n$; c'est ce qui sera évident, si de cette équation on peut tirer des valeurs entières de $Y$ et $Z$, quelles que soient les indéterminées $y$ et $z$ de la formule proposée.

Or de l'équation précédente on tire $4\Delta^n p^n = (2p^nY+\phi Z)^2 + aZ^2$ $= 4\left(\frac{(2py+qz)^2}{4}+\frac{az^2}{4}\right)^n$. Soit pour un moment $2p^nY+\phi Z=X$, $2py+qz=x$, on aura l'équation $X^2+aZ^2 = 4(\frac{1}{4}x^2+\frac{1}{4}az^2)^n$. Or on satisfait généralement à cette équation en prenant

$$(\tfrac{1}{2}x+\tfrac{1}{2}z\sqrt{-a})^n = \tfrac{1}{2}X+\tfrac{1}{2}Z\sqrt{-a};$$

et on sait que les nombres $X$ et $Z$ tirés de celle-ci seront toujours entiers; il reste donc à démontrer que $Y$ est aussi un entier. Or on a $2p^nY = X-\phi Z$ et $X^2+aZ^2 = 4\Delta^n p^n$; substituant dans la seconde, au lieu de $a$, sa valeur, $4p^n\psi-\phi^2$, on aura $X^2-\phi^2Z^2$ $= 4p^n(\Delta^n-\psi Z^2)$. Or on prouvera, comme ci-dessus, que les facteurs $X-\phi Z$, $X+\phi Z$ n'ont point de commun diviseur autre que 2; donc puisque $X^2-\phi^2Z^2$ est divisible par $p^n$, il faut que l'un des facteurs $X-\phi Z$, $X+\phi Z$ soit divisible par $p^n$, et comme on peut prendre à volonté le signe de $\phi$, on pourra représenter par $X-\phi Z$ celui des deux facteurs qui est divisible par $p^n$; il le sera en même temps par $2p^n$, parce que $\phi$ est impair; donc la quantité $Y = \frac{X-\phi Z}{2p^n}$ sera toujours un nombre entier, ou plutôt sera une fonction entière des indéterminées $y$ et $z$. Donc la formule $p^nY^2+\phi YZ+\psi Z^2$ représentera en général la puissance $n$ de la formule proposée $py^2+qyz+rz^2$.

*Remarque.* Si l'on veut simplement savoir à quelle forme des diviseurs quadratiques appartient la puissance $n$ d'un diviseur quadratique donné $\Delta$, l'opération se réduit à déterminer les coefficiens $\varphi$ et $\psi$, comme on l'a expliqué dans les deux cas; ensuite on ramènera à l'expression la plus simple la formule $p^n y^2 + 2\varphi yz + \psi z^2$, ou la formule $p^n y^2 + \varphi yz + \psi z^2$ (si $a$ est de la forme $8n+3$), qui contient la puissance désignée.

Il est facile maintenant d'évaluer dans les produits des quantités $A$, $B$, $C$, &c. (n°. 370) les termes qui contiennent des puissances de ces quantités.

### EXEMPLE I.

(373) Soit la formule $t^2 + 41u^2$ dont les cinq diviseurs quadratiques sont :

$$A = y^2 + 2yz + 42z^2 \qquad D = 3y^2 + 2yz + 14z^2$$
$$B = 2y^2 + 2yz + 21z^2 \qquad E = 6y^2 + 2yz + 7z^2.$$
$$C = 5y^2 + 6yz + 10z^2$$

Si on multiplie entre eux deux diviseurs, tels que $C$ et $D$ (en distinguant par des accens les indéterminées de l'un des deux), on trouvera (n°. 362) que le produit $CD$, réduit à l'expression la plus simple, est à-la-fois de la forme $D$ et de la forme $E$. On trouvera semblablement les autres résultats suivans qui renferment les formes des produits de deux diviseurs semblables ou dissemblables, dans toutes les combinaisons possibles : on y a joint les quarrés de ces mêmes diviseurs trouvés par les formules du n°. 367, ou par celles du n°. 371 :

| | | | | | |
|---|---|---|---|---|---|
| $A^2 = A$ | $AA = A$ | $BB = A$ | $CC = \left\{\begin{matrix}A\\B\end{matrix}\right.$ | $DD = \left\{\begin{matrix}A\\C\end{matrix}\right.$ | $EE = \left\{\begin{matrix}A\\C\end{matrix}\right.$ |
| $B^2 = A$ | $AB = B$ | $BC = C$ | | | |
| $C^2 = B$ | $AC = C$ | $BD = E$ | $CD = \left\{\begin{matrix}D\\E\end{matrix}\right.$ | $DE = \left\{\begin{matrix}B\\C\end{matrix}\right.$ | |
| $D^2 = C$ | $AD = D$ | $BE = D$ | | | |
| $E^2 = C$ | $AE = E$ | | $CE = \left\{\begin{matrix}D\\E\end{matrix}\right.$ | | |

De-là on déduira la forme du produit de tant de diviseurs qu'on voudra, où l'on pourra faire entrer des puissances supérieures à la seconde,

seconde, en cherchant la valeur par les formules du n°. 371. Par exemple, les produits des trois diviseurs semblables seront :

$$AAA = AA = A \qquad DDD = \begin{cases} AD \\ CD \end{cases} = \begin{cases} D \\ D \\ E \end{cases}$$

$$BBB = AB = B$$

$$CCC = \begin{cases} AC \\ BC \end{cases} = \begin{cases} C \\ C \end{cases} \qquad EEE = \begin{cases} AE \\ CE \end{cases} = \begin{cases} E \\ D \\ E \end{cases}$$

d'où l'on voit que le produit $BBB$ se réduit à la seule forme $B$; que le produit $CCC$ se réduit de deux manières différentes à la forme $C$; que le produit $DDD$ se réduit de deux manières à la forme $D$, et d'une manière à la forme $E$, &c. Dans le cas où les trois facteurs seroient égaux, les produits se réduiroient à une seule forme, et on auroit (n°. 371)

$$A^3 = A,\ B^3 = B,\ C^3 = C,\ D^3 = E,\ E^3 = D.$$

EXEMPLE II.

(374) Considérons encore la formule $t^2 + 89u^2$ qui a sept diviseurs quadratiques, savoir :

$$A = y^2 + 2yz + 90z^2 \qquad E = 7y^2 + 6yz + 14z^2$$
$$B = 2y^2 + 2yz + 45z^2 \qquad F = 3y^2 + 2yz + 30z^2$$
$$C = 9y^2 + 2yz + 10z^2 \qquad G = 6y^2 + 2yz + 15z^2.$$
$$D = 18y^2 + 2yz + 5z^2$$

Les combinaisons de ces diviseurs multipliés deux à deux, donnent les résultats suivans, auxquels on a joint les quarrés de ces mêmes diviseurs :

| | | | | | |
|---|---|---|---|---|---|
| $A^2 = A$ | $AA = A$ | $BB = A$ | $CC = \begin{cases} A \\ D \end{cases}$ | $DD = \begin{cases} A \\ D \end{cases}$ | $EE = \begin{cases} A \\ B \end{cases}$ |
| $B^2 = A$ | $AB = B$ | $BC = D$ | $CD = \begin{cases} E \\ C \end{cases}$ | $DE = \begin{cases} F \\ G \end{cases}$ | $EF = \begin{cases} C \\ D \end{cases}$ |
| $C^2 = D$ | $AC = C$ | $BD = C$ | $CE = \begin{cases} F \\ G \end{cases}$ | $DF = \begin{cases} E \\ G \end{cases}$ | $EG = \begin{cases} C \\ D \end{cases}$ |
| $D^2 = D$ | $AD = D$ | $BE = E$ | $CF = \begin{cases} E \\ F \end{cases}$ | $DG = \begin{cases} E \\ F \end{cases}$ | $FF = \begin{cases} A \\ C \end{cases}$ |
| $E^2 = B$ | $AE = E$ | $BF = G$ | $CG = \begin{cases} E \\ G \end{cases}$ | | $FG = \begin{cases} B \\ D \end{cases}$ |
| $F^2 = C$ | $AF = F$ | $BG = F$ | | | $GG = \begin{cases} A \\ C \end{cases}$ |
| $G^2 = C$ | $AG = G$ | | | | |

De-là on déduira aisément les formes des produits de tant de diviseurs qu'on voudra, ayant soin de prendre pour les puissances supérieures à la seconde les formes déterminées n°. 371. Par exemple, si on veut avoir toutes les formes des produits $A^2B$, $B^2C$, $C^2D$, &c., on trouvera

| | | | | | | |
|---|---|---|---|---|---|---|
| $A^2A=A$ | $B^2A=A$ | $C^2A=D$ | $D^2A=D$ | $E^2A=B$ | $F^2A=C$ | $G^2A=C$ |
| $A^2B=B$ | $B^2B=B$ | $C^2B=C$ | $D^2B=C$ | $E^2B=A$ | $F^2B=D$ | $G^2B=D$ |
| $A^2C=C$ | $B^2C=C$ | $C^2C=\begin{cases}B\\C\end{cases}$ | $D^2C=\begin{cases}B\\C\end{cases}$ | $E^2C=D$ | $F^2C=\begin{cases}A\\D\end{cases}$ | $G^2C=\begin{cases}A\\D\end{cases}$ |
| $A^2D=D$ | $B^2D=D$ | $C^2D=\begin{cases}A\\D\end{cases}$ | $D^2D=\begin{cases}A\\D\end{cases}$ | $E^2D=C$ | $F^2D=\begin{cases}B\\C\end{cases}$ | $G^2D=\begin{cases}B\\C\end{cases}$ |
| $A^2E=E$ | $B^2E=E$ | $C^2E=\begin{cases}F\\G\end{cases}$ | $D^2E=\begin{cases}F\\G\end{cases}$ | $E^2E=E$ | $F^2E=\begin{cases}F\\G\end{cases}$ | $G^2E=\begin{cases}F\\G\end{cases}$ |
| $A^2F=F$ | $B^2F=F$ | $C^2F=\begin{cases}E\\G\end{cases}$ | $D^2F=\begin{cases}E\\G\end{cases}$ | $E^2F=G$ | $F^2F=\begin{cases}E\\F\end{cases}$ | $G^2F=\begin{cases}E\\F\end{cases}$ |
| $A^2G=G$ | $B^2G=G$ | $C^2G=\begin{cases}E\\F\end{cases}$ | $D^2G=\begin{cases}E\\F\end{cases}$ | $E^2G=F$ | $F^2G=\begin{cases}E\\G\end{cases}$ | $G^2G=\begin{cases}E\\G\end{cases}$ |

Au moyen de ces développemens, on peut voir tout d'un coup quelles sont les combinaisons qui peuvent produire une forme déterminée. Ainsi on voit que $A$ résulte également des sept combinaisons $A^2A$, $B^2A$, $C^2A$, $D^2D$, $E^2B$, $F^2C$, $G^2C$; de sorte que si on avoit à résoudre l'équation $t^2+89u^2=x^2x'$, cette équation auroit sept solutions.

De même ayant trouvé $A^3=A$, $B^3=B$, $C^3=C$, $D^3=A$, $E^3=E$, $F^3=E$, $G^3=E$, on en conclura que l'équation $y^2+89z^2=x^3$ a deux solutions, que l'équation $7y^2+6yz+14z^2=x^3$ en a trois, que l'équation $18y^2+2yz+5z^2=x^3$ n'en a aucune, et ainsi des autres.

§. IV. *Résolution en nombres entiers de l'équation* $Ly^2+Myz+Nz^2=b\Pi$, $\Pi$ *étant le produit de plusieurs indéterminées ou de leurs puissances.*

(375) Soit $LN-\frac{1}{4}M^2=a$, si $M$ est pair, ou $4LN-M^2=a$, si $M$ est impair, il est aisé de voir que le premier membre de l'équation proposée sera un diviseur quadratique de la formule $t^2+au^2$, et cette équation elle-même étant multipliée par $L$ ou $4L$, deviendra de la forme $t^2+au^2=c\Pi$, $c$ étant $Lb$ ou $4Lb$. De-là il suit que tout facteur de $\Pi$ doit diviser la formule $t^2+au^2$, et par conséquent pourra être représenté par un diviseur quadratique de cette formule. C'est de ce principe, et de la théorie exposée dans le §. précédent, que nous déduirons la solution générale de l'équation dont il s'agit; mais d'abord il convient de débarrasser le second membre du facteur constant $c$.

Si dans l'équation $t^2+au^2=c\Pi$, on suppose $t$ et $u$ premiers entr'eux, il faudra que $u$ et $c$ le soient aussi, et alors on pourra faire $t=nu+cx$, ce qui donnera, après avoir substitué et divisé par $c$,

$$\left(\frac{n^2+a}{c}\right)u^2+2nux+cx^2=\Pi.$$

Or $u$ et $c$ sont premiers entr'eux, donc il faut que $n^2+a$ soit divisible par $c$, et en faisant $n^2+a=mc$, on aura

$$mu^2+2nux+cx^2=\Pi,$$

équation dont le second membre est dégagé du facteur constant $c$, et dont le premier est encore un diviseur quadratique de la formule $t^2+au^2$, puisqu'on a $mc-n^2=a$.

On aura donc autant de ces équations à résoudre, qu'il y aura de valeurs de $n$, moindres que $\frac{1}{2}c$, telles que $n^2+a$ soit divisible par $c$.

Soit $fy^2+2gyz+hz^2=\Pi$ l'équation ou l'une des équations qui restent à résoudre. Le premier membre étant un diviseur quadra-

tique de la formule $t^2+au^2$, il faudra d'abord chercher tous les diviseurs quadratiques de cette formule, que l'on désignera par les lettres $A$, $B$, $C$, $D$, &c. Ensuite comme $\Pi$ est supposé le produit de plusieurs indéterminées, on cherchera, par les méthodes précédentes, toutes les formes auxquelles se réduit le produit $\Pi$ en supposant que les indéterminées sont représentées par les lettres $A$, $B$, $C$, $D$, &c., suivant toutes les combinaisons possibles, et en observant que différentes indéterminées peuvent être désignées par la même lettre. Cela posé, parmi toutes ces formes on distinguera celles qui donnent pour résultat la lettre correspondante au diviseur quadratique du premier membre $fy^2+2gyz+hz^2$; et il est clair qu'autant on trouvera de ces formes, autant il y aura de solutions de l'équation $fy^2+2gyz+hz^2=\Pi$. Il faudra ensuite, pour obtenir réellement les solutions, faire le développement successif des produits suivant les règles que nous avons données dans le §. précédent, et alors les indéterminées $y$ et $z$ s'exprimeront finalement en fonctions des indéterminées analogues qui entrent dans les différens facteurs du produit $\Pi$. Tout cela s'éclaircira suffisamment par des exemples.

### EXEMPLE I.

(376) Soit proposée l'équation $t^2+41u^2=113x^2$; je développe d'abord tous les diviseurs quadratiques de $t^2+41u^2$, lesquels sont, comme on l'a déjà vu (n°. 373),

$$A=y^2+2yz+42z^2 \qquad D=3y^2+2yz+14z^2$$
$$B=2y^2+2yz+21z^2 \qquad E=6y^2+2yz+7z^2.$$
$$C=5y^2+6yz+10z^2$$

Parmi ces diviseurs, il n'y a que $A$, $B$, $C$ qui comprennent les nombres $4n+1$, et dans lesquels on pourra trouver 113. Or si le diviseur $A$ contenoit 113, il faudroit que 113 fût de la formule $t^2+41u^2$, ce qui n'a pas lieu, comme on le voit au premier coup d'œil; pareillement si le diviseur $B$ contenoit 113, il faudroit que $2\times113$ ou 226 fût de la forme $t^2+41u^2$; c'est encore ce qui n'a pas lieu. Comme cependant on peut voir, par le caractère $\left(\frac{41}{113}\right)=1$, que 113 est diviseur de $t^2+41u^2$, il s'ensuit que 113 est nécessaire-

ment compris dans le diviseur quadratique $C$; et en effet on a $5.113=565=14^2+41.3^2$. Puisque $14^2+41.3^2$ est divisible par 113, si l'on fait $14=3n-113m$, il faudra que $n^2+41$ soit divisible par 113. Or la valeur de $n$ tirée de cette équation est $n=-33$. On connoît donc ainsi, d'une manière directe et presque sans tâtonnement, la valeur de $n$ qui rend $n^2+41$ divisible par 113. Cette méthode, que nous venons d'exposer avec quelque détail, est un développement de celle du n°. 187.

Cela posé, soit $t=33u+113t'$, on aura, après avoir substitué et divisé par 113,

$$10u^2+66ut'+113t't'=x^2.$$

Pour réduire le premier membre à une expression plus simple, soit $u=u'-3t'$, on aura

$$5t't'+6t'u'+10u'u'=x^2.$$

Le premier membre étant de la forme $C$, il faut chercher parmi les valeurs de $A^2$, $B^2$, &c. celles qui peuvent être de la forme $C$; or on trouve (n°. 373) que $D^2$ et $E^2$ sont de cette forme; donc l'équation proposée est susceptible de deux solutions, selon que l'on supposera $x=D$ ou $x=E$.

Soit 1°. $x=3y^2+2yz+14z^2$, on trouvera par les formules du n°. 371, $x^2=5Y^2+6YZ+10Z^2$, les valeurs de $Y$ et $Z$ étant $Y=-y^2+4yz+6z^2$, $Z=y^2+2yz-4z^2$, de sorte qu'on aura en même temps $t'=Y$, $u'=Z$.

Soit 2°. $x=6y^2+2yz+7z^2$, le résultat de cette seconde valeur pourra se déduire facilement du précédent (en mettant $2y$ à la place de $y$, et divisant par 2 tant la valeur de $x$ que celles de $Y$ et $Z$); on aura ainsi $x^2=5Y^2+6YZ+10Z^2$, $Y=-2y^2+4yz+3z^2$, $Z=2y^2+2yz-2z^2$, et on fera de nouveau $t'=Y$, $u'=Z$.

Il reste à substituer les valeurs de $t'$ et $u'$ dans celles de $t$ et $u$; ce qui donnera les deux solutions suivantes de l'équation proposée

$$x=3y^2+2yz+14z^2,\ t=19y^2+122yz-48z^2,\ u=4y^2-10yz-22z^2$$
$$x=6y^2+2yz+7z^2,\ t=38y^2+122yz-24z^2,\ u=8y^2-10yz-11z^2.$$

## Exemple II.

(377) Proposons-nous maintenant l'équation $t^2+41u^2=113x^3$.

L'opération préliminaire pour diviser chaque membre par 113,

étant faite comme dans l'exemple précédent, on aura $t=33u'+14t'$, $u=u'-3t'$, et la transformée sera

$$5t't'+6t'u'+10u'u'=x^3.$$

Il faudra donc chercher les différentes formes des quantités $A^1$, $B^1$, $C^{II}$, &c., et voir si la forme $C$ y est comprise. Or on trouve (n°. 373) que la forme $C$ ne peut résulter que de $C^3$, et ainsi l'équation proposée n'est susceptible que d'une solution.

Maintenant si on fait $x=C=5y^2+6yz+10z^2$, on trouvera, d'après les formules du n°. 371, $\varphi=\pm 47$, $\psi=18$ et $x^3=125Y^2 \pm 94YZ+18Z^2$. Quant aux valeurs de $Y$ et $Z$, elles doivent être déduites des équations $125Y\pm 47Z=x^3-123xz^2$, $Z=3x^2z-41z^3$, où l'on a $x=5y+3z$; or pour que $Y$ soit une fonction entière, on trouve qu'il faut dans les signes ambigus prendre l'inférieur, et alors on a

$$Y=y^3+30y^2z+30yz^2-8z^3$$
$$Z=75y^2z+90yz^2-14z^3$$
$$x^3=125Y^2-94YZ+18Z^2.$$

La valeur de $x^3$ se réduit à l'expression la plus simple $5t't'+6t'u'+10u'u'$ en faisant $Z=3Y-u'$, puis $Y=t'+2u'$, de sorte qu'on aura $u'=3Y-Z=3y^3+15y^2z-10z^3$, $t'=2Z-5Y=-5y^3+30yz^2+12z^3$. Donc enfin la solution de l'équation proposée est comprise dans les formules

$$x=5y^2+6yz+10z^2$$
$$t=29y^3+495y^2z+420yz^2-162z^3$$
$$u=18y^3+15y^2z-90yz^2-46z^3.$$

## EXEMPLE III.

(378) Si on propose en général l'équation $t^2+2u^2=113x^m$, la manière la plus simple de la résoudre, est de faire $x=y^2+2z^2$, $113=9^2+2.4^2$; et on aura $t^2+2u^2=(9^2+2.4^2)(y^2+2z^2)^m$. Or on satisfait généralement à cette équation, en prenant

$$t+u\sqrt{-2}=(9\pm 4\sqrt{-2})(y+z\sqrt{-2})^m.$$

Soit donc $(y+z\sqrt{-2})^m=Y+Z\sqrt{-2}$, on aura $t+u\sqrt{-2}=(9\pm 4\sqrt{-2})(Y+Z\sqrt{-2})$, partant

$$t=9Y\mp 8Z$$
$$u=9Z\pm 4Y.$$

C'est la seule solution dont l'équation proposée soit susceptible, parce que $x$, comme diviseur de $t^2+2u^2$, ne peut avoir que la seule forme $y^2+2z^2$.

### EXEMPLE IV.

(379) L'équation $t^2+89u^2=x^3$, doit avoir deux solutions, ainsi que nous l'avons déjà remarqué à la fin du n°. 374. L'une des solutions où l'on aura $x=y^2+89z^2$, se trouve immédiatement par l'équation $t^2+89u^2=(y^2+89z^2)^3$, à laquelle on satisfait en faisant $t+u\sqrt{-89}=(y+z\sqrt{-89})^3$; et ainsi on aura $t=y^3-267yz^2$, $u=3y^2z-89z^3$. La seconde solution, fondée sur ce que $D^3=\mathcal{A}$, se trouvera comme il suit.

Ayant fait $x=D=5y^2+2yz+18z^2$; si l'on applique à ce cas particulier les formules du n°. 371, on aura $p=5$, $q=1$, $r=18$, $\varphi=6$, $\psi=1$, ce qui donnera

$$x^3=125Y^2+12YZ+Z^2$$
$$Y=y^3-3y^2z-12yz^2+2z^3$$
$$Z=75y^2z+30yz^2-86z^3.$$

Or on peut mettre la valeur de $x^3$ sous la forme $x^3=(Z+6Y)^2+89Y^2$, laquelle étant comparée à l'équation proposée, donnera $t=Z+6Y$, $u=Y$; donc enfin la seconde solution de cette équation sera donnée par les formules

$$x=5y^2+2yz+18z^2$$
$$t=6y^3+57y^2z-42yz^2-74z^3$$
$$u=y^3-3y^2z-12yz^2+2z^3.$$

### EXEMPLE V.

(380) On a déjà remarqué (n°. 374) que l'équation $t^2+89u^2=x^2x'$ doit avoir sept solutions, attendu que la forme $\mathcal{A}$ résulte des sept combinaisons $\mathcal{A}^2\mathcal{A}$, $B^2\mathcal{A}$, $C^2D$, $D^2D$, $E^2B$, $F^2C$, $G^2C$. Pour développer une de ces solutions, prenons la combinaison $C^2D$, et faisons en conséquence $x=9y^2+2yz+10z^2$, $x'=5y'^2+2y'z'+18z'^2$, on trouvera d'abord par les formules du n°. 367, ou par celles du n°. 371

$$x^2=5T^2+2TV+18V^2$$
$$T=y^2-8yz+2z^2$$
$$V=2y^2+2yz-2z^2.$$

Si ensuite on multiplie la valeur de $x^2$ par celle de $x'$, on trouvera par la première des deux formules du n°. 367,

$$x^2x' = (5Ty' + Tz' + Vy' + 18Vz')^2 + 89(Tz' - Vy')^2.$$

Comparant ce résultat avec l'équation proposée $t^2 + 89u^2 = x^2x'$, on aura

$$t = 5Ty' + Tz' + Vy' + 18Vz'$$
$$u = Tz' - Vy';$$

d'où l'on voit que les quatre indéterminées $t$, $u$, $x$, $x'$ sont exprimées eu fonctions de quatre autres indéterminées indépendantes $y$, $z$, $y'$, $z'$, ce qui constituera la première solution. On trouvera par des calculs semblables les six autres solutions dont l'équation proposée est susceptible.

*Remarque.* Pour peu qu'on y fasse attention, on verra que cette théorie s'étendroit facilement au cas où le premier membre de l'équation proposée seroit un diviseur de la formule $t^2 - au^2$. On pourroit aussi résoudre, par les mêmes principes, le cas où les indéterminées du premier membre seroient supposées avoir un diviseur commun; mais nous n'avons pas cru devoir entrer dans tous ces détails, qui n'offrent maintenant aucune difficulté.

---

§. V.

## §. V. *Démonstration d'une propriété relative aux diviseurs quadratiques de la formule* $t^2+au^2$, *a étant un nombre premier* $8n+1$.

On a déjà remarqué, n°. 215, que si dans la formule $t^2+au^2$, $a$ est un nombre de forme $8n+5$, deux diviseurs conjugués de cette formule, tels que $py^2+2qyz+2mz^2$, $2py^2+2qyz+mz^2$, appartiendront toujours l'un à la forme $4n+1$, l'autre à la forme $4n-1$; de sorte qu'alors il y a autant de diviseurs quadratiques $4n+1$ que de diviseurs $4n-1$, et ce résultat a lieu quel que soit le nombre $a$, pourvu qu'il ne sorte pas de la forme $8n+5$.

Au contraire, lorsque $a$ est de forme $8n+1$, les deux diviseurs conjugués dont il s'agit sont tous deux de la forme $4n+1$, ou tous deux de la forme $4n-1$, de sorte qu'on ne peut plus rien conclure sur le nombre relatif des uns et des autres, et en effet l'inspection de la Table IV fait voir qu'il y a à cet égard une grande irrégularité. Mais lorsque $a$ est un nombre premier, on remarque dans cette même Table que le nombre des diviseurs quadratiques $4n+1$ surpasse constamment d'une unité le nombre des diviseurs $4n-1$. Ainsi on voit que la formule $t^2+41u^2$ a trois diviseurs quadratiques $4n+1$, et seulement deux $4n-1$; que la formule $t^2+89u^2$ a quatre diviseurs quadratiques $4n+1$, et seulement trois $4n-1$, &c.

On s'assurera aisément de cette propriété dans beaucoup d'autres cas particuliers; mais il n'est pas aussi facile de l'établir d'une manière générale et rigoureuse. Voici la série de propositions que cette démonstration semble exiger : elles offriront en même temps divers résultats remarquables qui contribueront à étendre et perfectionner les théories précédentes.

(381) Proposition I. *Soit* a *un nombre premier* $4n+1$, *et soit* $py^2+2qyz+2mz^2$ *un diviseur quadratique* $4n+1$, *de la formule*

$t^2+au^2$, *je dis que l'équation* $U^2=py^2+2qyz+2mz^2$ *sera toujours résoluble.*

Car si l'on multiplie cette équation par $p$, et qu'on fasse $py+qz=x$, on aura $pU^2=x^2+az^2$, équation toujours possible (Voyez nos. 27 et 196).

Il est inutile d'observer que si $py^2+2qyz+2mz^2$ étoit un diviseur $4n-1$, l'équation $U^2=py^2+2qyz+2mz^2$ seroit impossible, puisqu'aucun quarré ne peut être de la forme $4n-1$.

(382) Proposition II. a *étant un nombre premier* $8n+1$, *la formule* $t^2+au^2$ *aura toujours un diviseur quadratique de la forme* $fy^2+2gyz+2fz^2$.

Car on peut toujours (no. 147) satisfaire à l'équation $a=2f^2-g^2$, laquelle étant posée, il s'ensuit que $fy^2+2gyz+2fz^2$, ou l'expression la plus simple de cette formule, est un diviseur quadratique de la formule $t^2+au^2$.

*Remarquez* que le diviseur $fy^2+2gyz+2fz^2$ ne diffère pas de son conjugué; dans ce cas, par conséquent, les deux diviseurs conjugués se réduisent en un seul, qu'on peut appeler *diviseur singulier*.

(383) Proposition III. a *étant un nombre premier* $8n+1$, *il y a toujours une infinité de valeurs de* f *et de* g *qui satisfont à l'équation* $2f^2-g^2=a$, *néanmoins il n'en peut résulter qu'un seul diviseur quadratique de la formule* $t^2+au^2$.

Car on trouvera aisément (no. 38) que la série des valeurs de $f$ et $g$ qui satisfont à l'équation $2f^2-g^2=a$, est telle que si $f'$ et $g'$ suivent immédiatement $f$ et $g$, on a

$$f'=3f+2g,\ g'=3g+4f.$$

De ces nouvelles valeurs résulte le diviseur quadratique singulier

$$(3f+2g)y^2+2(3g+4f)yz+2(3f+2g)z^2.$$

Or si dans ce diviseur on fait $y=2z'-y'$, $z=y'-z'$, (ce qui ne restreint pas la généralité des variables $y$ et $z$), on aura pour transformée $fy'^2+2gy'z'+2fz'^2$; d'où l'on voit qu'en effet le diviseur quadratique $f'y^2+2g'yz+2f'z^2$ n'est pas différent de $fy^2+2gyz+2fz^2$.

*Corollaire.* De-là il suit que $a$ étant un nombre premier $8n+1$, les diviseurs quadratiques de la formule $t^2+au^2$ seront composés de plusieurs couples de diviseurs conjugués et d'un diviseur singulier. Le nombre total de ces diviseurs sera donc toujours impair, et ainsi il est impossible que le nombre des diviseurs $4n+1$ soit égal au nombre des diviseurs $4n-1$.

(384) PROPOSITION IV. *Le quarré d'un diviseur quadratique* $py^2+2qyz+2\pi z^2$, *et celui de son conjugué* $2py^2+2qyz+\pi z^2$, *sont compris dans un même diviseur quadratique* $p^2y^2+2\varphi yz+\psi z^2$.

Car suivant la méthode du n°. 367, si l'on détermine $\mu$ et $\nu$ par l'équation $\pi=p\mu-q\nu$, qu'ensuite on fasse $\varphi=q+\nu p$, $\psi=\nu^2+2\mu$, $Y=y^2-2\nu yz-2\mu z^2$, $Z=2z(py+qz)$, on aura

$$(py^2+2qyz+2\pi z^2)^2=p^2Y^2+2\varphi YZ+\psi Z^2.$$

Dans cette équation, qui doit être identique, mettons $2y$ à la place de $y$, et comme alors $Y$ devient pair, ainsi que $Z$, faisons $Y=2Y'$, $Z=2Z'$, ce qui donnera $Y'=2y^2-2\nu yz-\mu z^2$, $Z'=z(2py+qz)$, nous aurons par la substitution, et après avoir divisé par 4,

$$(2py^2+2qyz+\pi z^2)^2=p^2Y'^2+2\varphi Y'Z'+\psi Z'^2.$$

Donc le même diviseur quadratique $p^2y^2+2\varphi yz+\psi z^2$, qui contient le quarré du diviseur $py^2+2qyz+2\pi z^2$, contient aussi le quarré de son conjugué $2py^2+2qyz+\pi z^2$.

*Corollaire.* Étant proposée l'équation $U^2=PY^2+2QYZ+RZ^2$, si on en connoît une solution comprise dans la formule $U=py^2+2qyz+2\pi z^2$, il y aura toujours une autre solution donnée par la forme conjuguée $U=2py^2+2qyz+\pi z^2$. Ces deux solutions se confondent en une seule, si la valeur de $U$ est égale au diviseur quadratique singulier, c'est-à-dire si l'on a $U=fy^2+2gyz+2fz^2$; mais alors le second membre de l'équation proposée seroit de la forme $2Y^2+2YZ+\left(\frac{a+1}{2}\right)Z^2$.

(385) PROPOSITION V. p *étant un nombre premier, ainsi que* a, *si l'on a* $p^2=M^2+aN^2$, *je dis que* p *ou* 2p *sera nécessairement*

*de la même forme* $t^2+au^2$, *de sorte que* p *appartiendra soit au diviseur quadratique* $y^2+2yz+(a+1)z^2$, *soit à son conjugué* $2y^2+2yz+\left(\frac{a+1}{2}\right)z^2$.

En effet, l'équation supposée $p^2=M^2+aN^2$, donne $p^2-M^2=aN^2$; donc puisque $a$ est un nombre premier, il faut que l'un des facteurs $p+M$, $p-M$ soit divisible par $a$, et comme le signe de $M$ peut être pris à volonté, on pourra faire $p+M=aP$, $p-M=Q$, ce qui donnera $PQ=N^2$. Or on satisfait généralement à cette dernière équation, en faisant, avec de nouvelles indéterminées, $P=\pi^2R$, $N=\pi\omega R$, $Q=\omega^2R$. On aura donc $2p=aP+Q=R(\omega^2+a\pi^2)$, d'où l'on voit que $R$ ne peut être que 1 ou 2: si $R=2$, on aura $p=\omega^2+a\pi^2$; si $R=1$, on aura $2p=\omega^2+a\pi^2$. Donc $p$ ou $2p$ est nécessairement de la forme $t^2+au^2$. Mais si $p$ est de la forme $t^2+au^2$, il est contenu dans le diviseur quadratique $y^2+az^2$, qui est le même que $y^2+2yz+(a+1)z^2$, et il ne peut par conséquent appartenir qu'à ce seul diviseur. De même si $2p$ est de la forme $t^2+au^2$, $p$ appartiendra au diviseur quadratique $2y^2+2yz+\left(\frac{a+1}{2}\right)z^2$, et il ne pourra appartenir qu'à ce seul diviseur. Donc si on a $p^2=M^2+aN^2$, il faudra que $p$ appartienne à l'un des diviseurs conjugués $y^2+2yz+(a+1)z^2$, $2y^2+2yz+\left(\frac{a+1}{2}\right)z^2$.

(386) Proposition VI. p *étant un nombre premier quelconque, et* a *un nombre premier* $8n+1$, *si l'on a* $p^2=2M^2+2MN+\left(\frac{a+1}{2}\right)N^2$, *c'est-à-dire si* $2p^2$ *est de la forme* $P^2+aN^2$, *je dis que* p *appartiendra nécessairement au diviseur quadratique singulier* $fy^2+2gyz+2fz^2$, *en sorte qu'on aura* $p=f\mu^2+2g\mu\nu+2f\nu^2$.

Car $a$ étant un nombre premier $8n+1$, on peut faire $a=2f^2-g^2$, et cette valeur étant substituée dans l'équation $2p^2=P^2+aN^2$, il en résultera $2(p^2-f^2N^2)=P^2-g^2N^2$. Or j'observe que les nombres $P$, $N$ doivent être impairs, ainsi que $f$, $g$; d'où il suit que non-seulement les deux facteurs $p+fN$, $p-fN$ sont tous deux pairs, mais que leur produit $p^2-f^2N^2$ est divisible par 8.

Il faut donc que l'un de ces facteurs soit divisible par 4, & l'autre par 2 seulement : car s'ils étoient tous deux divisibles par 4, leur somme $2p$ seroit aussi divisible par 4, ce qui est impossible, $p$ étant un nombre premier impair. Maintenant comme le signe de $f$ est arbitraire, nous pourrons supposer que le facteur $p-fN$ est celui qui n'est divisible que par 2. Un semblable raisonnement ayant lieu à l'égard des facteurs $P+gN$, $P-gN$, on supposera de même que $P-gN$ est divisible par 2 seulement. Or de l'équation $2(p^2-f^2N^2)=P^2-g^2N^2$, on tire $\frac{P-gN}{p-fN}=\frac{2(p+fN)}{P+gN}$; soit $\frac{\beta}{\gamma}$ l'expression la plus simple de l'une et l'autre fractions ; $\beta$ et $\gamma$ seront impairs, et il faudra qu'on ait, en prenant deux nouvelles arbitraires $\alpha$, $\delta$,

$$P-gN=2\alpha\beta \qquad 2(p+fN)=4\beta\delta$$
$$p-fN=2\alpha\gamma \qquad P+gN=4\gamma\delta.$$

De-là on tire $p=\alpha\gamma+\beta\delta$, ensuite $fN=\beta\delta-\alpha\gamma$, $gN=2\gamma\delta-\alpha\beta$; donc $f(2\gamma\delta-\alpha\beta)=g(\beta\delta-\alpha\gamma)$, ou

$$\frac{\beta}{\gamma}=\frac{2f\delta+g\alpha}{f\alpha+g\delta}.$$

La fraction $\frac{\beta}{\gamma}$ étant déjà réduite à ses moindres termes, cette équation ne peut subsister à moins qu'on n'ait $2f\delta+g\alpha=\beta H$, $f\alpha+g\delta=\gamma H$, $H$ étant une indéterminée. De-là on tire, à cause de $a=2f^2-g^2$,

$$a\alpha=H(2f\gamma-g\beta)$$
$$a\delta=H(f\beta-g\gamma).$$

Or $\alpha$ et $\delta$ sont premiers entr'eux, sans quoi $\alpha\gamma+\beta\delta$ ou $p$ ne seroit pas un nombre premier ; donc on peut satisfaire à l'équation $m\alpha-n\delta=1$. Mais en vertu des deux équations précédentes, $a\alpha$ et $a\delta$ étant divisibles chacun par $H$, la quantité $ma\alpha-na\delta$, égale à $a$, sera aussi divisible par $H$. Donc $H$ ne peut être que 1 ou $a$.

Soit 1°. $H=1$, on aura $\beta=2f\delta+g\alpha$, $\gamma=f\alpha+g\delta$; donc $\alpha\gamma+\beta\delta$ ou $p=f\alpha^2+2g\alpha\delta+2f\delta^2$. Donc $p$ est compris dans le diviseur singulier $fy^2+2gyz+2fz^2$.

Soit 2°. $H=a$, on aura $\alpha=2f\gamma-g\zeta$, $\delta=f\zeta-g\gamma$; donc $\alpha\gamma+\zeta\delta$ ou $p=f\zeta^2-2g\zeta\gamma+2f\gamma^2$; donc $p$ est encore compris dans le diviseur singulier $fy^2+2gyz+2fz^2$.

(387) PROPOSITION VII. *Je dis maintenant que les deux diviseurs conjugués qui pris pour U satisfont à l'équation proposée* $v^2=PY^2+2QYZ+RZ^2$, *sont les seules solutions dont cette équation soit susceptible.*

Pour démontrer cette proposition, cherchons en général les conditions qui doivent avoir lieu pour que deux valeurs différentes de $U$ savoir :

$$U=py^2+2qyz+2\pi z^2$$
$$U=p'y^2+2q'yz+2\pi' z^2$$

satisfassent également à l'équation proposée $U^2=PY^2+2QYZ+RZ^2$ où $Y$ et $Z$ sont des indéterminées qui doivent être fonctions des indéterminées $y$ et $z$.

Nous supposerons que les deux valeurs de $U$ sont préparées de manière que $p$ et $p'$ soient des nombres premiers; cela posé, on trouvera d'abord que les quarrés de ces valeurs sont compris dans deux formules de cette sorte :

$$p^2y^2+2\varphi yz+\psi z^2$$
$$p'^2y^2+2\varphi' yz+\psi' z^2,$$

lesquelles doivent se réduire, l'une et l'autre, à la forme donnée $Py^2+2Qyz+Rz^2$. De-là on voit que $p^2$ doit être compris dans la formule $p'^2y^2+2\varphi'yz+\psi'z^2$, et réciproquement $p'^2$ dans la formule $p^2y^2+2\varphi yz+\psi z^2$. On peut donc faire tout à-la-fois

$$p^2=p'^2\alpha'^2+2\varphi'\alpha'\zeta'+\psi'\zeta'^2.$$
$$p'^2=p^2\alpha^2+2\varphi\alpha\zeta+\psi\zeta^2.$$

Soit $p^2\alpha+\varphi\zeta=\gamma$, $p'^2\alpha'+\varphi'\zeta'=\gamma'$, on aura

$$p^2p'^2=\gamma^2+a\zeta^2=\gamma'^2+a\zeta'^2,$$

partant $\gamma^2-\gamma'^2=a(\zeta'^2-\zeta^2)$. Mais puisque $a$ est un nombre premier, et qu'on peut prendre à volonté le signe de $\gamma'$ et celui de $\zeta'$, on satisfera généralement à cette équation, en faisant

$$\gamma+\gamma'=a\Delta B \qquad \zeta'+\zeta=\Delta C$$
$$\gamma-\gamma'=CD \qquad \zeta'-\zeta=BD,$$

$A, B, C, D$ étant des indéterminées. De là on tire $2y = aAB + CD$, $2z = AC - BD$, et par conséquent $4y^2 + 4az^2$, ou

$$4p^2p'^2 = (aA^2 + D^2)(aB^2 + C^2).$$

Par la forme du premier membre, on voit d'abord que le second doit être divisible par 4. Or on ne peut faire que deux suppositions par rapport aux deux facteurs $aA^2 + D^2$, $aB^2 + C^2$; ou l'un d'eux, par exemple $aA^2 + D^2$, sera divisible par 4, et alors il faudra que les deux nombres $A$ et $D$ soient pairs; ou les deux facteurs $aA^2 + D^2$, $aB^2 + C^2$ seront divisibles l'un et l'autre par 2, ce qui suppose les nombres $A$, $B$, $C$, $D$ tous impairs. Dans le premier cas, si l'on fait $A = 2A'$, $D = 2D'$, on aura

$$p^2p'^2 = (aA'^2 + D'^2)(aB^2 + C^2).$$

Dans le second cas, soit $D = A + 2M$, $C = B + 2N$, on aura

$$p^2p'^2 = \left(2M^2 + 2AM + \frac{a+1}{2}A^2\right)\left(2N^2 + 2BN + \frac{a+1}{2}B^2\right).$$

Enfin puisque $p$ et $p'$ sont des nombres premiers, ces deux équations ne peuvent se décomposer ultérieurement que suivant un certain nombre de combinaisons, lesquelles se réduisent à six, savoir :

$$\begin{array}{l|l}
(1) & p^2 = aB^2 + C^2, \quad p'^2 = aA'^2 + D'^2 \\
(2) & p = aB^2 + C^2, \quad pp'^2 = aA'^2 + D'^2 \\
(3) & pp' = aB^2 + C^2 = aA'^2 + D'^2 \\
(4) & p^2 = 2M^2 + 2MA + \frac{a+1}{2}A^2, \quad p'^2 = 2N^2 + 2NB + \frac{a+1}{2}B^2 \\
(5) & p = 2M^2 + 2MA + \frac{a+1}{2}A^2, \quad pp'^2 = 2N^2 + 2NB + \frac{a+1}{2}B^2 \\
(6) & pp' = 2M^2 + 2MA + \frac{a+1}{2}A^2 = 2N^2 + 2NB + \frac{a+1}{2}B^2.
\end{array}$$

Dans la première combinaison, il faut, suivant la Prop. V, que $p$ et $p'$ soient compris dans le diviseur quadratique $y^2 + 2yz + (a+1)z^2$, ou dans son conjugué $2y^2 + 2yz + \left(\frac{a+1}{2}\right)z^2$; mais comme ils ne peuvent appartenir tous deux au même diviseur quadratique, parce

qu'alors les deux valeurs de $U$ se réduiroient à une seule, il s'ensuit que les nombres $p$ et $p'$ sont compris, l'un dans le diviseur quadratique $y^2+2yz+(a+1)z^2$, l'autre dans son conjugué $2y^2+2yz+\frac{1}{2}(a+1)z^2$. Si l'on observe d'ailleurs que le nombre $p$, qui est supposé premier, ne peut appartenir qu'à un seul diviseur quadratique, et qu'il en est de même du nombre $p'$, on verra que cette première combinaison suppose que les deux valeurs de $U$ qui satisfont à l'équation proposée sont :

$$U=y+2yz+(a+1)z^2$$
$$U=2y^2+2yz+\left(\frac{a+1}{2}\right)z^2.$$

Alors l'équation proposée seroit de la forme $U^2=Y^2+2YZ+(a+1)Z^2$.

Dans la deuxième combinaison, on voit 1°. que le nombre $p$ appartient à la forme $y^2+2yz+(a+1)z^2$; 2°. que puisque $pp'^2=aA'^2+D'^2$, il faut que $p$ et $p'^2$ appartiennent à un même diviseur quadratique (n°. 231) : mais $p'^2$ et $p^2$ sont compris aussi dans le même diviseur quadratique, donc il faudra que $p$ et $p^2$ soient compris dans le même diviseur, qui par conséquent ne pourra être que $y^2+2yz+(a+1)z^2$. Quant à $p'$, son quarré devant être compris dans cette même forme, il faudra que $p'$ ou $2p'$ y soit aussi compris. Or $p'$ ne peut l'être, parce qu'alors $p$ et $p'$ seroient compris dans un même diviseur quadratique, et par conséquent les deux valeurs de $U$ se réduiroient à une seule, ce qui est contre la supposition. Donc il faudra supposer que $2p'$ est compris dans le diviseur $y^2+2yz+(a+1)z^2$; c'est-à-dire que $p'$ est compris dans le diviseur $2y^2+2yz+(a+1)z^2$. On retombe donc dans le même résultat qu'a déjà présenté la première combinaison.

Dans la troisième combinaison, les nombres $p$ et $p'$ appartiendroient à un même diviseur quadratique, et ainsi les deux valeurs de $U$ coincideroient en une seule, ce qui est contre la supposition.

Dans la quatrième combinaison, on voit, d'après la Prop. VI, que les nombres $p$ et $p'$ appartiendroient à un même diviseur quadratique, qui seroit le diviseur singulier $fy^2+2gyz+2fz^2$; donc les deux valeurs de $U$ se réduiroient encore à une seule, ce qui est contre la supposition.

Dans

Dans la cinquième combinaison, on voit 1°. que le nombre $p$ appartient au diviseur quadratique $2y^2+2yz+\frac{a+1}{2}z^2$; 2°. que les nombres $2p$ et $p'^2$ appartiennent à un même diviseur quadratique; mais $p'^2$, ainsi que $p^2$, appartient au diviseur $y^2+2yz+(a+1)z^2$, et alors $2p$ appartient à ce même diviseur. Donc pour concilier ces conditions, il faut que $p$ appartenant au diviseur $2y^2+2yz+\frac{a+1}{2}z^2$, $p'$ appartienne à son conjugué $y^2+2yz+(a+1)z^2$, ce qui rentrera dans la première combinaison.

Enfin, dans la sixième combinaison, il faut que les nombres $p$ et $2p'$ appartiennent à un même diviseur quadratique; cela prouve que le diviseur quadratique qui contient $p$ et celui qui contient $p'$, doivent être deux diviseurs conjugués. En effet, soit $py^2+2qyz+2\pi z^2$ le diviseur quadratique qui contient $p$; comme ce diviseur doit contenir aussi $2p'$, il pourra être mis sous la forme $2p'y^2+2kyz+hz^2$, mais alors son conjugué, qui est $p'y^2+2kyz+2hz^2$, contient $p'$. Donc comme $p'$ ne peut appartenir qu'à un seul diviseur quadratique, il appartiendra nécessairement au diviseur conjugué de $py^2+2qyz+2\pi z^2$, lequel est sous une autre forme $2py^2+2qyz+\pi z^2$.

De la considération de tous ces cas, il suit manifestement qu'étant proposée l'équation $U^2=PY^2+2QYZ+RZ^2$, dans laquelle le second membre est l'un des diviseurs quadratiques de la formule $t^2+au^2$, où $a$ est un nombre premier $8n+1$, cette équation n'admettra jamais que deux solutions, ou deux valeurs de $U$, lesquelles seront représentées par les deux diviseurs conjugués $U=py^2+2qyz+2\pi z^2$, $U=2py^2+2qyz+\pi z^2$. Et ces deux valeurs se réduiront même à une seule $U=fy^2+2gyz+2fz^2$, si l'équation proposée est de la forme $U^2=2Y^2+2YZ+\left(\frac{a+1}{2}\right)Z^2$.

(388) Proposition VIII. *Le nombre des diviseurs quadratiques* $4n+1$ *de la formule* $t^2+au^2$, *où* $a$ *est un nombre premier* $8n+1$, *surpasse toujours d'une unité le nombre des diviseurs quadratiques* $4n-1$ *de la même formule.*

En effet, soit $M$ le nombre des diviseurs quadratiques $4n+1$,

et $N$ le nombre des diviseurs quadratiques $4n-1$; si on désigne par $A$, $B$, $C$, $D$, &c. la suite des diviseurs quadratiques $4n+1$, les équations $U^2=A$, $U^2=B$, $U^2=C$, &c. admettront chacune deux solutions distinctes, à l'exception de l'équation $U^2=2Y^2+2YZ+\frac{a+1}{2}Z^2$, qui n'en admettra qu'une. Donc le nombre total des solutions sera $2M-1$. Mais ces solutions qui doivent être toutes distinctes les unes des autres, comprennent nécessairement tous les diviseurs quadratiques, tant $4n+1$ que $4n-1$, de la formule $t^2+au^2$. Donc on aura $2M-1=M+N$, ou $N=M-1$ : c'est la proposition qu'il s'agissoit de démontrer.

---

## §. VI. *Méthodes pour compléter la résolution en nombres entiers des équations indéterminées du second degré.*

(389) Nous avons donné dans la première partie les méthodes nécessaires pour résoudre en nombres entiers les équations indéterminées du second degré, qui sont de la forme $ay^2+byz+cz^2=H$; c'est en effet à cette forme que peut être réduite toute équation proposée du second degré; mais il reste une condition à remplir lorsque l'équation dont il s'agit contient des termes du premier degré.

Soit en général $ay^2+byz+cz^2+dy+fz+g=0$ l'équation proposée; pour faire disparoître les termes où les indéterminées sont au premier degré, je fais $y=\frac{y'+\alpha}{\theta}$, $z=\frac{z'+\beta}{\theta}$, et j'ai la transformée

$$\begin{aligned}0=ay'^2+by'z'+cz'^2&+2a\alpha y'+2c\beta z'+a\alpha^2+d\alpha\theta\\&+\ b\beta y'+b\alpha z'+b\alpha\beta+f\beta\theta\\&+\ d\theta y'+f\theta z'+c\beta^2+g\theta^2.\end{aligned}$$

Supposant donc $2a\alpha+b\beta+d\theta=0$, $2c\beta+b\alpha+f\theta=0$, on aura $\frac{\alpha}{\theta}=\frac{2cd-fb}{bb-4ac}$, $\frac{\beta}{\theta}=\frac{2af-db}{bb-4ac}$; d'où l'on voit que si dans l'équation proposée on fait immédiatement

$$y=\frac{y'+2cd-fb}{bb-4ac}\,,\qquad z=\frac{z'+2af-db}{bb-4ac}\,,$$

la transformée sera

$$ay'^2+by'z'+cz'^2=-(af^2-bdf+cd^2)(bb-4ac)-g(bb-4ac)^2.$$

Je remarque maintenant qu'on peut supposer que les coefficiens $a$, $b$, $c$ des termes du second degré dans l'équation proposée, n'ont pas de diviseur commun; car s'ils avoient un commun diviseur $\omega$, il faudroit que $dy+fz+g$ fût aussi divisible par $\omega$; or cette condition est facile à remplir, en introduisant une indéter-

minée nouvelle à la place de $y$ ou de $z$, et alors toute l'équation devient divisible par $\omega$.

Je remarque aussi qu'on peut faire abstraction du cas où $bb-4ac$ est une quantité négative, parce qu'alors le nombre des solutions de la transformée étant toujours limité, le procédé le plus simple est de substituer successivement les valeurs trouvées de $y'$ et $z'$ dans les formules $y=\frac{y'+2cd-fb}{bb-4ac}$, $z=\frac{z'+2af-db}{bb-4ac}$, afin de voir quelles sont celles qui donnent pour $y$ et $z$ des nombres entiers.

On peut se dispenser encore de discuter le cas où $b^2-4ac$, quoique positif, seroit égal à un quarré, parce qu'alors la transformée n'a encore qu'un nombre de solutions limité (n°. 70). Il ne reste donc à examiner que le cas où $bb-4ac$ est un nombre positif non-quarré.

(390) Alors la transformée, si elle est résoluble, aura toujours une infinité de solutions renfermées dans un ou plusieurs systêmes, et chaque systême pourra être représenté par les formules

$$y'=\gamma F+\delta G$$
$$z'=\epsilon F+\zeta G$$
$$[\varphi+\psi\sqrt{(bb-4ac)}]^n=F+G\sqrt{(bb-4ac)}.$$

Pour éviter la considération des cas particuliers, nous supposerons que ces formules sont préparées de manière que les nombres $\gamma$, $\delta$, $\epsilon$, $\zeta$, $\varphi$, $\psi$ sont des entiers, et que l'exposant $n$ est un nombre à volonté. Quelquefois la solution immédiate donnera, pour ces coefficiens, des nombres affectés de la fraction $\frac{1}{2}$; il pourra arriver aussi que l'exposant $n$ soit d'une forme désignée paire ou impaire. Mais dans tous les cas, il est facile de réduire les formules à la forme que nous supposons, où tous les nombres sont entiers et l'exposant $n$ à volonté : il faut de plus se rappeler qu'on aura toujours $\varphi^2-\psi^2(b^2-4ac)=1$.

Cela posé, il s'agit de trouver en général la valeur de $n$ telle que les quantités

$$y=\frac{\gamma F+\delta G+\alpha}{bb-4ac}, \quad z=\frac{\epsilon F+\zeta G+6}{bb-4ac}$$

soient des entiers. Or on a

$$F = \varphi^n + \frac{n.n-1}{1.2}\varphi^{n-2}\psi^2(bb-4ac) + \&c.$$

$$G = n\varphi^{n-1}\psi + \frac{n.n-1.n-2}{1.2.3}\varphi^{n-3}\psi^3(bb-4ac) + \&c.$$

Ainsi en substituant les valeurs de $F$ et $G$, on voit que la question se réduit à déterminer $n$ de manière que les quantités $\frac{\gamma\varphi^n + \delta n\varphi^{n-1}\psi + \alpha}{bb-4ac}$, $\frac{\varepsilon\varphi^n + \zeta n\varphi^{n-1}\psi + \beta}{bb-4ac}$, soient des entiers. Pour cela, nous distinguerons deux cas, selon que $n$ est pair ou impair.

Soit 1°. $n = 2m$, l'équation $\varphi^2 - \psi^2(b^2 - 4ac) = 1$, donne, en négligeant les multiples de $b^2 - 4ac$, $\varphi^{2m} = 1$; on peut donc, au lieu de $\alpha$ et $\beta$, mettre $\alpha\varphi^{2m}$ et $\beta\varphi^{2m}$, et alors supprimant le facteur $\varphi^{2m}$ qui ne peut avoir aucun diviseur commun avec $b^2 - 4ac$, on trouve que la détermination de $m$ ne dépend plus que des équations du premier degré

$$\frac{(\alpha+\gamma)\varphi + 2\delta\psi m}{bb-4ac} = e, \quad \frac{(\beta+\varepsilon)\varphi + 2\zeta\psi m}{bb-4ac} = e,$$

lesquelles doivent s'accorder entr'elles, pour que l'équation proposée soit résoluble en nombres entiers.

Soit 2°. $n = 2m + 1$, alors, en négligeant les multiples de $bb - 4ac$, on aura encore $\alpha = \alpha\varphi^{2m}$ et $\beta = \beta\varphi^{2m}$, et la détermination de $m$ dépendra des équations du premier degré

$$\frac{\gamma\varphi + \alpha + (2m+1)\delta\psi}{bb-4ac} = e, \quad \frac{\varepsilon\varphi + \beta + (2m+1)\zeta\psi}{bb-4ac} = e,$$

lesquelles doivent encore s'accorder entr'elles.

Donc dans tous les cas on trouvera les valeurs convenables de l'exposant $n$ par la simple résolution d'une équation indéterminée du premier degré, et la valeur de $n$ qui résultera de cette solution étant en général de la forme $v + (bb - 4ac)k$, où $k$ est une indéterminée, il s'ensuit qu'on aura une infinité de valeurs de $n$ qui satisferont à la question, de sorte qu'on aura aussi une infinité de solutions de l'équation proposée en nombres entiers. On doit d'ailleurs observer que les nombres $F$ et $G$ peuvent être pris chacun avec le signe qu'on voudra, ce qui donnera quatre combi-

naisons à examiner séparément, et d'où pourront résulter différentes solutions.

(391) Soit proposé maintenant, pour compléter cette théorie, de résoudre la question suivante :

*Les nombres* F *et* G *étant donnés par la formule* $(\varphi+\psi\sqrt{A})^n = F+G\sqrt{A}$, *dans laquelle l'exposant* n *est indéterminé, et où l'on a* $\varphi^2-\psi^2 A=1$, *trouver toutes les valeurs de* n *telles que la quantité* $\lambda F+\mu G+\nu$ *soit divisible par un nombre premier* $\omega$, *qui ne divise pas* $A\psi$.

Voici une méthode qui a été indiquée pour cet objet par Lagrange (Mém. de Berlin, 1767).

Je suppose d'abord qu'on connoisse une valeur de l'exposant $n$ qui satisfait à la question ; soit cette valeur $p$, il faudra qu'en faisant $(\varphi+\psi\sqrt{A})^p=f+g\sqrt{A}$, la quantité $\frac{\lambda f+\mu g+\nu}{\omega}$ soit un entier. Je cherche ensuite un exposant $q$, tel qu'en faisant $(\varphi+\psi\sqrt{A})^q=f'+g'\sqrt{A}$, le nombre $g'$ soit divisible par $\omega$. Il est certain que cet exposant existe, puisqu'on peut toujours satisfaire à l'équation $x^2-A\omega^2y^2=1$. Cet exposant étant trouvé, on peut supposer en même temps que $f'-1$ soit divisible par $\omega$ ; si cela n'étoit pas, on doubleroit l'exposant $q$ ; et faisant $(\varphi+\psi\sqrt{A})^{2q}$ ou $(f'+g'\sqrt{A})^2=f''+g''\sqrt{A}$, on auroit $f''=f'^2+Ag'^2=1+2Ag'^2$, et $g''=2f'g'$, de sorte que $f'-1$ et $g''$ seroient à-la-fois divisibles par $\omega$. Donc en faisant les préparations convenables, on trouvera toujours un exposant $q$, tel qu'en faisant $(\varphi+\psi\sqrt{A})^q=f'+g'\sqrt{A}$, les nombres $f'-1$ et $g'$ soient l'un et l'autre divisibles par $\omega$.

Je dis maintenant qu'en prenant $n=qx+p$, la quantité proposée $\lambda F+\mu G+\nu$ sera divisible par $\omega$, quel que soit l'entier $x$. Car soit $(f'+g'\sqrt{A})^x=F'+G'\sqrt{A}$, on aura $F+G\sqrt{A} =(f+g\sqrt{A})\,(F'+G'\sqrt{A})$, d'où l'on tire $F=fF'+gAG'$, $G=fG'+gF'$, et $\lambda F+\mu G+\nu=(\lambda f+\mu g)F'+(\lambda gA+\mu f)G'+\nu$. Mais les valeurs développées de $F'$ et $G'$ étant $F'=f'^x+\frac{x.x-1}{1.2}f'^{x-2}g'^2A+$ &c., $G'=nf'^{x-1}g'+$ &c., si on néglige les multiples de $\omega$, on aura $G'=0$, et $F'=f'^x=1$ ; donc en négli-

geant les mêmes multiples, la quantité $\lambda F+\mu G+\nu$ se réduit à $\lambda f+\mu g+\nu$, donc elle est divisible par $\omega$.

Puisque toutes les valeurs de $n$ comprises dans la formule $n=qx+p$ satisfont à la question, il y aura toujours une de ces valeurs qui sera moindre que $q$, de sorte qu'on pourra toujours supposer $p<q$. Donc pour avoir l'exposant $p$ qui donne la première solution, il faut élever $\varphi+\psi\sqrt{A}$ à ses puissances successives $0, 1, 2, 3 \ldots q-1$, et essayer, pour chaque puissance représentée par $f+g\sqrt{A}$, si la quantité $\lambda f+\mu g+\nu$ est divisible par $\omega$. On peut aussi former directement la suite des quantités $\lambda f+\mu g$, en observant que cette suite est récurrente, et qu'elle a pour échelle de relation $2\varphi$, $-1$; d'où il suit qu'au moyen des deux premiers termes connus $\lambda$, $\lambda\varphi+\mu\psi$, on formera aisément tous les autres. Ces calculs sont d'autant plus faciles, qu'on peut rejeter les multiples de $\omega$, à mesure qu'ils se présentent, et si le problême est possible, il faudra que dans les $q$ premiers termes de la suite dont il s'agit, on trouve une ou plusieurs fois $\lambda f+\mu g+\nu=0$.

(392) Connoissant l'exposant le plus petit $p$ qui rend $\lambda f+\mu g+\nu$ divisible par un nombre premier $\omega$, voici la méthode qu'on peut suivre pour trouver *a priori* une valeur de $n$, telle que $\lambda F+\mu G+\nu$ soit divisible par une puissance donnée de $\omega$.

Nous observerons d'abord, qu'on peut résoudre généralement l'équation $\dfrac{L+Mx+N\omega+P\omega^2+Q\omega^3+\text{\&c.}}{\omega^m}=e$, dans laquelle $L$ et $M$ sont des nombres donnés, et $N$, $P$, $Q$, &c. des fonctions quelconques entières de $x$. Pour cela, il faudra déterminer $x$ de manière que $\dfrac{L+Mx}{\omega}$ soit un entier; ayant trouvé $x=l+\omega x'$, si on substitue cette valeur dans l'équation proposée, elle deviendra de la forme $\dfrac{L'+M'x'+N'\omega+P'\omega^2+Q'\omega^3+\text{\&c.}}{\omega^{m-1}}=e$ semblable à la proposée, mais dont le dénominateur est d'un degré moindre d'une unité. On aura donc, par une suite de procédés semblables, $x=l+\omega x'$, $x'=l'+\omega x''$, $x''=l''+\omega x'''$, &c.; d'où l'on conclura

$x = l + l'\omega + l''\omega^2 + l'''\omega^3 +$ &c. jusqu'à un terme de la forme $\omega^m x^{(m)}$ dans lequel $x^{(m)}$ sera une nouvelle indéterminée.

Cela posé, si l'on veut, par exemple, déterminer la valeur de $n$ telle que la quantité $\lambda F + \mu G + \nu$ soit divisible par $\omega^3$, on fera comme ci-dessus $n = qx + p$, et toutes choses étant d'ailleurs les mêmes, faisant de plus $\lambda f + \mu g = \lambda'$, $\lambda g \mathcal{A} + \mu f = \mu'$, on aura $\lambda F + \mu G + \nu = \lambda' F' + \mu' G' + \nu$. Dans cette quantité, qui est déjà divisible par $\omega$, quel que soit $x$, il faudra substituer, au lieu de $F'$ et $G'$ leurs valeurs développées, en omettant la troisième puissance et les puissances supérieures de $g'$; ces valeurs sont :

$$F' = f'^x + \frac{x \cdot x-1}{2} f'^{x-2} g'^2 \mathcal{A}, \quad G' = x f'^{x-1} g'.$$

On distinguera ensuite deux cas, selon que $x$ est pair ou impair.

1°. Si $x$ est pair, on pourra, à la place de $\nu$, mettre $\nu(f'^2 - g'^2 \mathcal{A})^{\frac{x}{2}}$, et développer cette quantité, en omettant les termes qui contiennent $g'^3$ et les puissances supérieures de $g'$. Par ces substitutions, l'équation proposée $\dfrac{\lambda' F' + \mu' G' + \nu}{\omega^3} = e$ deviendra

$$\frac{\lambda'\left(f'^x + \frac{x \cdot x-1}{1 \cdot 2} f'^{x-2} g'^2 \mathcal{A}\right) + \mu' \cdot x f'^{x-1} g' + \nu\left(f'^x - \frac{x}{2} \cdot f'^{x-2} g'^2 \mathcal{A}\right)}{\omega^3} = e.$$

Or $f'$ n'étant pas divisible par $\omega$, puisque $f' - 1$ l'est, on peut supprimer du numérateur le facteur commun $f'^{x-2}$, ce qui fait disparoître la variable en exposant ; si de plus on fait $g' = \omega h'$, $\lambda' + \nu = \omega L$, l'équation à résoudre deviendra

$$\frac{L f'^2 + \mu' f' h' x + \left(\lambda' \cdot \frac{x \cdot x-1}{1 \cdot 2} - \nu \frac{x}{2}\right) h'^2 \mathcal{A} \omega}{\omega^2} = c.$$

Et celle-ci pouvant se traiter par la méthode précédente, on aura le résultat de la forme $x = l + l'\omega + \omega^2 x''$, où il faudra prendre l'indéterminée $x''$ de manière que $x$ soit pair.

2°. Si $x$ est impair, il faudra, à la place de $\nu$, mettre $\nu(f'^2 - g'^2 \mathcal{A})^{\frac{x-1}{2}}$, et d'ailleurs le calcul sera entièrement semblable à celui du premier cas.

On voit maintenant le procédé à suivre, pour faire en sorte qu'une

qu'une quantité de la forme $\lambda F + \mu G + \nu$ soit divisible par un nombre quelconque $P$. Ayant décomposé $P$ en ses facteurs premiers, soit $\omega^m$ un de ses facteurs, on cherchera les valeurs de $n$, telles que la quantité proposée soit divisible par $\omega^m$, et ainsi successivement par rapport à chacun des autres facteurs. On aura différentes valeurs particulières de $n$ qu'il faudra combiner ensemble, afin d'avoir une valeur générale qui satisfasse à toutes les conditions, et le problème ne sera résoluble qu'autant que toutes ces conditions pourront être remplies.

(393) Nous remarquerons que la valeur de $q$ dont on a besoin dans la solution précédente (n°. 391), peut être donnée directement par le théorême suivant.

*Si l'on a* $\varphi^2 - \mathrm{A}\psi^2 = 1$, *et qu'on cherche un exposant* q, *tel que* $(\varphi + \psi\sqrt{\mathrm{A}})^q - 1$ *soit divisible par un nombre premier* $\omega$ *non diviseur de* $\mathrm{A}\psi$, *je dis qu'on peut faire* $\mathrm{q} = \omega - 1$ *si l'on a* $\left(\frac{\mathrm{A}}{\omega}\right) = +1$, *et* $\mathrm{q} = \omega + 1$ *si l'on a* $\left(\frac{\mathrm{A}}{\omega}\right) = -1$.

En effet on trouvera, comme au n°. 129, que la quantité $(\varphi + \psi\sqrt{A})^\omega - (\varphi + \psi\sqrt{A})$, divisée par $\omega$, laisse le même reste qu'une quantité semblable $(\varphi - k + \psi\sqrt{A})^\omega - (\varphi - k + \psi\sqrt{A})$, dans laquelle $k$ est un entier quelconque. Soit $k = \varphi$, on aura ainsi, en omettant les multiples de $\omega$,

$$(\varphi + \psi\sqrt{A})^\omega - (\varphi + \psi\sqrt{A}) = (\psi\sqrt{A})^\omega - \psi\sqrt{A},$$

et le second membre, à cause de $\psi^\omega = \psi$, devient $\psi\sqrt{A}\left(A^{\frac{\omega-1}{2}} - 1\right)$ ou $\psi\sqrt{A}\left[\left(\frac{A}{\omega}\right) - 1\right]$.

Soit 1°. $\left(\frac{A}{\omega}\right) = 1$, on aura $(\varphi + \psi\sqrt{A})^\omega - (\varphi + \psi\sqrt{A}) = 0$, donc $(\varphi + \psi\sqrt{A})^{\omega - 1} - 1$ est divisible par $\omega$, donc on peut faire $q = \omega - 1$.

Soit 2°. $\left(\frac{A}{\omega}\right) = -1$, on aura $(\varphi + \psi\sqrt{A})^\omega = \varphi - \psi\sqrt{A}$, donc $(\varphi + \psi\sqrt{A})^{\omega + 1} = \varphi^2 - A\psi^2 = 1$, donc on peut faire $q = \omega + 1$.

---

## §. VII. *Méthode de Fermat pour la résolution de l'équation* $y^2 = a + bx + cx^2 + dx^3 + ex^4$ *en nombres rationnels.*

(394) Ayant été conduits à traiter fort au long de la résolution des équations indéterminées, nous devons faire mention d'une méthode indiquée par Fermat pour résoudre en nombres rationnels l'équation $y^2 = a + bx + cx^2 + dx^3 + ex^4$, dont le second membre est un polynome rationnel où la variable ne passe pas le quatrième degré. Voici les cas principaux dans lesquels la résolution est possible.

1°. Si le nombre $a$ est égal à un quarré positif $f^2$, les valeurs $x = 0$, $y = f$ donneront immédiatement une solution de l'équation proposée. Pour avoir une autre solution, on supposera $a + bx + cx^2 + dx^3 + ex^4 = (f + gx + hx^2)^2$, ce qui donnera, en développant et ordonnant,

$$\begin{array}{l} 0 = f^2 + 2fgx + 2fhx^2 + 2ghx^3 + h^2x^4 \\ \quad\; -a \quad -b \quad\;\; + g^2 \quad\;\; -d \quad\;\; -e \\ \qquad\qquad\qquad\;\; -c. \end{array}$$

Or on a déjà $f^2 = a$; si pour faire disparoître les deux termes suivans, on fait $2fg - b = 0$, $2fh + g^2 - c = 0$, on en tirera les valeurs des coefficiens $g$ et $h$, lesquelles seront $g = \frac{b}{2f}$, $h = \frac{c - g^2}{2f}$. Alors l'équation étant réduite aux seuls termes qui contiennent $x^3$ et $x^4$, il en résultera une valeur rationnelle de $x$, savoir $x = \frac{2gh - d}{e - h^2}$. Cette valeur donnera donc une nouvelle solution en nombres rationnels de l'équation proposée; si toutefois on n'a pas $2gh = d$, ni $e = h^2$.

La nouvelle solution étant désignée par $x = m$, si l'on fait généralement $x = m + x'$, et qu'on substitue cette valeur dans l'équation proposée, le second membre deviendra de la forme $a' + b'x' + c'x'^2 + d'x'^3 + e'x'^4$, dans laquelle $a'$ sera encore un quarré positif.

On procédera donc de la même manière pour trouver une nouvelle valeur de $x'$, et ainsi à l'infini. D'où l'on voit qu'une première valeur connue de $x$ suffit pour en faire trouver une infinité d'autres, sauf quelques cas particuliers qui ne peuvent guère avoir lieu que lorsqu'il est absolument impossible de résoudre l'équation proposée autrement que par les premières valeurs données.

2°. Si le coefficient $e$ du terme $ex^4$ est égal à un quarré positif $h^2$, on fera $a+bx+cx^2+dx^3+ex^4=(f+gx+hx^2)^2$, ce qui donnera, en développant et réduisant,

$$\begin{array}{rllll} o = & f^2 & +2fgx & +2fhx^2 & +2ghx^3 \\ & -a & -b & +g^2 & -d \\ & & & -c & \end{array}$$

Maintenant on peut faire disparoître les $x^2$ et $x^3$, en prenant $g=\frac{d}{2h}$, $f=\frac{c-g^2}{2h}$, et alors l'équation réduite au premier degré, donne $x=\frac{a-f^2}{2fg-b}$. Cette solution en fournira ensuite une infinité d'autres comme dans le cas précédent, mais il faut qu'on n'ait pas $2fg-b=o$.

3°. Si l'équation proposée est de la forme $y^2=f^2+bx+cx^2+dx^3+h^2x^4$, en sorte qu'elle tombe à-la-fois dans les deux cas précédens, on pourra faire usage de chacun des moyens indiqués. On peut aussi tout d'un coup faire $y=f+gx\pm hx^2$, ce qui donnera, en substituant, développant et réduisant,

$$\begin{array}{rlll} o = & 2fgx & \pm 2fhx^2 & \pm 2ghx^3 \\ & -b & +g^2 & -d \\ & & -c & \end{array}$$

Or on peut satisfaire à celle-ci de deux manières, soit en faisant $g=\frac{b}{2f}$, ce qui donne $x=\frac{c-g^2\mp 2fh}{\pm 2gh-d}$, soit en faisant $g=\pm\frac{d}{2h}$, d'où l'on tire $x=\frac{2fg-b}{c-g^2\mp 2fh}$.

4°. Si on a une solution désignée par $x=m$, on fera $x=m+x'$, et l'équation sera ramenée au premier cas.

Nous pourrons ajouter un grand nombre d'applications de cette

méthode tirées des problêmes d'analyse indéterminée, dont Euler a donné les solutions dans plusieurs de ses Mémoires, et dans le second volume de son Algèbre. Nous nous bornerons à un ou deux exemples de ce genre, afin de donner une idée de cette branche d'analyse, qui exige une grande sagacité dans le choix des moyens de solution, mais qui n'a qu'un rapport éloigné avec notre sujet.

(395) Proposons-nous de trouver trois nombres $x, y, z$, tels que les trois formules

$$x^2+y^2+2z^2\ ,\quad x^2+z^2+2y^2\ ,\quad y^2+z^2+2x^2$$

soient égales à des quarrés.

Comme on peut supposer que ces nombres sont premiers entr'eux, il est aisé de voir qu'ils doivent être tous trois impairs: on peut donc faire $y=x+2p$, $z=x+2q$, et on aura

$$x^2+y^2+2z^2=4x^2+4(p+2q)x+4(p^2+2q^2).$$

Je fais cette quantité $=4(x+f)^2$, et j'en tire $x=\dfrac{p^2+2q^2-f^2}{2f-p-2q}$.

La seconde formule donnera semblablement $x=\dfrac{q^2+2p^2-g^2}{2g-q-2p}$,

et pour faire accorder ces deux valeurs, je fais

$$p^2+2q^2-f^2=q^2+2p^2-g^2\ ,\quad 2f-p-2q=2g-q-2p;$$

j'en tire des valeurs rationnelles de $f$ et de $g$, savoir $f=\frac{1}{4}(5q+3p)$, $g=\frac{1}{4}(5p+3q)$, au moyen desquelles la valeur de $x$ deviendra

$$x=\frac{7p^2-30pq+7q^2}{8(p+q)}.$$

Cette valeur satisfait déjà aux deux premières conditions : on aura d'ailleurs les valeurs correspondantes de $y$ et $z$ par les formules $y=x+2p$, $z=x+2q$; de sorte qu'en supprimant le facteur commun, on pourra faire

$$x=7p^2-30pq+7q^2$$
$$y=23p^2-14pq+7q^2$$
$$z=7p^2-14pq+23q^2.$$

Substituant ces valeurs dans la formule $y^2 + z^2 + 2x^2$, et faisant $\frac{p}{q} = 1 + \theta$, il restera à satisfaire à la condition

$$1 + 2\theta + 2\theta^2 + \theta^3 + \tfrac{169}{256}\theta^4 = \text{ à un quarré.}$$

Or on trouve immédiatement $\theta = 0$, ou $\theta = -1$, ou $\theta = -2$; mais il ne résulte de-là aucune solution. Soit donc, suivant la méthode précédente,

$$1 + 2\theta + 2\theta^2 + \theta^3 + \tfrac{169}{256}\theta^4 = (1 + \alpha\theta + \tfrac{13}{16}\theta^2)^2;$$

si l'on développe cette équation, et qu'on prenne $\alpha = \frac{8}{13}$, on aura $\theta = 208$; donc $p = 209$, $q = 1$, ce qui donne cette solution :

$$x = 18719, \quad y = 62609, \quad z = 18929.$$

Il seroit facile d'en trouver plusieurs autres, mais elles seroient probablement plus composées, quoique la méthode dont nous avons fait usage ne prouve pas que les nombres trouvés sont les moindres possibles qui satisfont à la question.

(396) Soit proposé encore de trouver trois quarrés inégaux $x^2$, $y^2$, $z^2$, tels que les trois formules $x^2 + y^2 - z^2$, $x^2 + z^2 - y^2$, $y^2 + z^2 - x^2$, soient égales à des quarrés.

On trouve aisément que les deux premières conditions sont remplies, en faisant

$$x = r^2 + s^2$$
$$y = r^2 + rs - s^2$$
$$z = r^2 - rs - s^2.$$

Il reste donc à satisfaire à la troisième, laquelle devient, par la substitution de ces valeurs, $r^4 - 4r^2s^2 + s^4 =$ à un quarré. Soit $r = \theta s$, la question se réduit à faire en sorte que $\theta^4 - 4\theta^2 + 1$ soit un quarré. On pourroit prendre $\theta = 0$, ou $\theta = 2$, mais il ne résulte de-là aucune solution convenable; pour avoir d'autres valeurs, soit $\theta = 2 + \varphi$, on aura $1 + 16\varphi + 20\varphi^2 + 8\varphi^3 + \varphi^4 =$ à un quarré. Je fais cette quantité $= (1 + 8\varphi + \alpha\varphi^2)^2$; prenant ensuite $\alpha = 1$, je trouve $\varphi = -\frac{23}{4}$; donc $\theta = -\frac{15}{4}$, $r = 15$, $s = 4$; d'où résulte cette solution :

$$x = 241, \quad y = 269, \quad z = 149.$$

Ce sont vraisemblablement les moindres nombres qui satisfont à

la question. On auroit pu faire encore $\alpha = -22$, ce qui auroit donné $\varphi = \frac{120}{161}$; $\theta = \frac{442}{161}$, ou $r = 442$, $s = 161$ : mais de-là résultent des nombres beaucoup plus considérables que les précédens.

On peut suivre un autre procédé pour faire en sorte que la quantité $1 + 16\varphi + 20\varphi^2 + 8\varphi^3 + \varphi^4$ soit égale à un quarré. Représentons ce quarré par $(1 + m\varphi + n\varphi^2)^2$, nous aurons, en comparant et développant,

$$\begin{array}{lllll} 0 = & 2m\varphi & +2n\varphi^2 & +2mn\varphi^3 & +n^2\varphi^4 \\ & -16 & +m^2 & -8 & -1 \\ & & -20 & & \end{array}$$

Soit $\varphi = \dfrac{16 - 2m}{2n + m^2 - 20} = \dfrac{8 - 2mn}{n^2 - 1}$, on aura entre $m$ et $n$ l'équation

$$(8 + m)n^2 + (m^3 - 20m - 8)n - 4m^2 + m + 72 = 0.$$

Maintenant pour avoir une valeur rationnelle de $n$, soit $m = -8$, on aura $n = -\frac{8}{15}$, $\varphi = \frac{120}{161}$, ce qui est la seconde des deux solutions trouvées par l'autre méthode.

*Nota.* Nous nous proposions d'ajouter à cette partie quelques autres objets intéressans, tels que le traité *de partitione numerorum*, composant l'un des plus beaux chapitres de l'*Introd. in Anal. inf.*, les Recherches de Lagrange sur les fonctions indéterminées dont les produits donnent des fonctions semblables, et un choix des plus beaux problêmes indéterminés résolus par Euler; mais l'étendue de cet ouvrage passant déjà les bornes que nous nous étions prescrites, nous sommes obligés de renvoyer pour ces objets aux ouvrages originaux.

# ADDITIONS.

*Introduction, art. X.*

La formule de cet article, corrigée d'une faute qui s'y est glissée, doit être lue ainsi :

$$(1+\alpha+\alpha^2\ldots\ldots+\alpha^m)(1+\beta+\beta^2\ldots\ldots+\beta^n)(1+\gamma+\gamma^2\ldots\ldots+\gamma^p)\,\&c.$$

On a déjà déduit de cette formule le nombre des diviseurs d'un nombre composé quelconque $N=\alpha^m\beta^n\gamma^p\ldots$ Mais il est évident qu'elle donne aussi la somme de ces mêmes diviseurs, $N$ compris. Voici une application de cette formule considérée sous ce nouveau point de vue.

Etant proposé de trouver deux nombres $A$ et $B$ tels que chacun d'eux soit égal à la somme des diviseurs de l'autre, cherchez parmi les puissances de 2 un nombre $a=2^\mu$ tel qu'en faisant $3a-1=b$, $6a-1=c$, $18a^2-1=d$, les nombres $b$, $c$, $d$, soient premiers; cette puissance étant trouvée (autre que $2^0$ ou 1) les nombres demandés seront $A=2^{\mu+1}d$, $B=2^{\mu+1}bc$.

En effet, soit $\int A$ la somme des diviseurs de $A$, $A$ non compris, et $\int B$ une somme semblable pour $B$, on aura, d'après la formule précédente, et parce que $1+2^1+2^2\ldots+2^{\mu+1}=2^{\mu+2}-1$,

$$\int A=(2^{\mu+2}-1)(1+d)-2^{\mu+1}d=(4a-1)18a^2-2a(18a^2-1)=B$$
$$\int B=(2^{\mu+2}-1)(1+b)(1+c)-2^{\mu+1}bc=(4a-1)18a^2-2a(3a-1)(6a-1)=A.$$

Donc les nombres $A$ et $B$ satisfont aux conditions du problême : mais cette solution est subordonnée à la possibilité de trouver pour $b$, $c$, $d$, des nombres premiers. On en a du moins un exemple, en faisant $a=2$, ce qui donne $A=284$, $B=220$.

Descartes est auteur de la solution de ce problême. Voyez le Tome III de ses Lettres, et le discours de Genty, intitulé *Influence de Fermat sur son siècle*, pag. 123.

*Introduction, art. XXVI.*

Le produit $\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{6}{7}\cdot\frac{10}{11}\ldots$ &c. prolongé suffisamment, devient moindre que toute quantité donnée. Car suivant le n°. 273 de l'*Introd. in Anal. inf.* on a

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\text{ \&c.}=\frac{1}{\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\text{ \&c.}}$$

Or le premier membre, égal à $-\log(1-x)$ dans le cas de $x=1$, est infini; donc le produit $\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)$ &c. continué à l'infini, est infiniment petit ou nul.

De-là et de la formule du n°. XXIV, il suit que s'il y a $p$ nombres premiers compris dans la suite des nombres naturels, depuis 1 jusqu'à $n$, le rapport de $p$ à $n$ diminuera de plus en plus, à mesure que $n$ augmente, et deviendra enfin moindre que toute fraction donnée.

*Introduction, art. XXVIII.*

Si on cherche, d'après les mêmes formules, combien il y a de nombres premiers de 1 à 10000, on trouvera que ce nombre $=5000\times0{,}240577+26=1229$; or le nombre effectif a été trouvé de 1230, d'après la vérification faite sur une table de nombres premiers. L'accord ne peut être plus satisfaisant, et doit faire présumer que le résultat trouvé pour les nombres premiers de 1 à 100000 est fort près de la vérité.

*Première Partie, §. XII.*

Puisque suivant le n°. 53 la valeur de $D$ a pour limite $2\sqrt{A}$, ou $\sqrt{(g^2-4fh)}$, il paroît qu'on peut rendre plus générale la proposition du §. XII, en l'étendant à toutes les valeurs de $H$ depuis zéro jusqu'à $\sqrt{(g^2-4fh)}$. C'est ce qui mérite d'être examiné.

*Seconde Partie*, n°. 230.

Fermat ayant avancé que le produit de deux nombres premiers compris dans les formes $20x+3$, $20x+7$ est toujours de la forme $y^2+5z^2$, il est facile de vérifier cette proposition par la Table IV. En

En effet les deux nombres dont il s'agit sont diviseurs de la formule $t^2+5u^2$, leur produit doit donc être diviseur de cette même formule ; mais ce produit sera toujours de l'une des formes linéaires $20x+1$, $20x+9$, donc il sera en même temps de la forme quadratique $y^2+5z^2$. On prouveroit la même chose plus directement par la formule $(2m^2+2mn+3n^2)(2p^2+2pq+3q^2)$ $=(2pm+pn+qm-2qn)^2+5(qm+pn+qn)^2$.

*Troisième Partie*, n°. 273.

Les trois équations $f\mu\nu=5$, $g\nu\lambda=9$, $h\lambda\mu=15$, suffisent pour déterminer à-la-fois les six quantités $\lambda, \mu, \nu, f, g, h$. Car $\lambda, \mu, \nu$ représentent les diviseurs communs entre deux des trois nombres $5, 9, 15$; on a donc d'abord $\lambda=3, \mu=5, \nu=1$. On trouve ensuite $f=1$, $g=3$, $h=1$.

*Troisième Partie, Théorême X.*

Il faut bien observer que l'exception $c^2=y^2+Nz^2$ doit être limitée elle-même par la condition que $z$ ne soit pas zéro, sans quoi l'exception comprendroit tous les cas, et le théorême deviendroit illusoire. En effet $z$ étant la même chose que ce qui est appelé $\varphi$ dans le cours de la démonstration, si on faisoit $\varphi=0$, on auroit $\gamma'\mathfrak{C}-\gamma\mathfrak{C}'=0$, $\alpha'\gamma-\alpha\gamma'=0$. De-là, à cause de $c=\alpha^2+\mathfrak{C}^2+\gamma^2=\alpha'^2+\mathfrak{C}'^2+\gamma'^2$, on concluroit $\alpha=\alpha'$, $\mathfrak{C}=\mathfrak{C}'$, $\gamma=\gamma'$; donc on auroit aussi $\lambda=\lambda'$, $\mu=\mu'$, $\nu=\nu'$, $A=A'$, $B=B'$, $C=C'$; de sorte que les deux formes de $N$ que l'on compare, seroient déduites d'un seul et même diviseur quadratique $\lambda^2x^2+\mu^2x'^2+\nu^2x''^2$, avec les mêmes valeurs des indéterminées. Ces formes ne seroient donc pas, comme on le suppose, le résultat de deux combinaisons différentes.

*Troisième Partie, Théorême XVI.*

Le Théorême XVI, considéré en lui-même et dans ses conséquences multipliées, est, sans aucun doute, une des plus belles et des plus fécondes propositions de la théorie des nombres : mais sa démonstration qui d'abord paroît suivre immédiatement du Théorême VIII, présente successivement des difficultés que nous n'avons pu lever entièrement, et qui exigent des recherches ultérieures.

On a démontré rigoureusement, n°. 318, que le Théorème XVI a lieu pour tout diviseur proposé $cy^2+2byz+az^2$, si parmi les nombres moindres que $N$ compris dans ce diviseur, il y a seulement un nombre $c$ qui n'ait aucun facteur quarré commun avec $N$, et qui en même temps ne satisfasse pas à l'équation $c^2=y^2+Nz^2$ où $z$ doit être $> 0$. La difficulté consiste donc à s'assurer *a priori* qu'il existe toujours un pareil nombre dans tout diviseur réciproque proposé.

La première condition est toujours facile à remplir, ainsi que nous l'avons fait voir n°. 320; quant à la seconde, il n'est pas nécessaire qu'elle le soit dans toute son étendue. Car quand même on auroit l'équation $c^2=y^2+Nz^2$, si les deux valeurs trinaires de $c$ qui ont conduit à cette équation (n°. 292) sont différentes, le fondement de la démonstration du n°. 318 subsistera dans son entier, puisque les deux combinaisons qui donnent les valeurs trinaires correspondantes de $N$ et de $c$ sont différentes l'une de l'autre, et doivent se retrouver telles dans les diviseurs de $t^2+Nu^2$. Les seuls cas, par conséquent, qui peuvent nuire au succès de la démonstration du n°. 318, sont ceux où le même diviseur quadratique de $t^2+cu^2$, dans deux formes trinaires qui répondent à une même valeur trinaire de $c$, et dans deux suppositions différentes pour les indéterminées qui le composent, donneroit deux formes trinaires identiques pour le nombre $N$.

En poussant plus loin ces considérations, on pourroit peut-être apporter quelque perfectionnement à la démonstration du Théorème XVI; mais pour rendre cette démonstration absolument complète, il restera toujours à examiner le cas où le quarré du diviseur proposé seroit de la forme $y^2+Nz^2$. Car quoique nous ayons prouvé que ce cas particulier rentre dans ceux des n$^{os}$ 313 et 314, il faut observer que la démonstration de ceux-ci suppose que le nombre auxiliaire $c$ ou $2b$ n'a point de facteur quarré; et c'est dans cette supposition seulement que la note de la page 377 est exacte: autrement on pourroit satisfaire à l'équation $4b^2=\varphi^2+N\psi^2$, en prenant toujours $\psi=1$, et ensuite $b=m^2$, $2a=5m^2-n^2$, $N=2ab-bb=m^2(4m^2-n^2)$. Il y auroit donc alors une infinité d'exceptions à la démonstration des Cas I et II, lesquels influent sur les autres Cas.

De là on voit que pour éviter toute difficulté, il paroît indispensable de chercher par une propositiou subsidiaire, combien de fois le nombre $N$ peut être contenu daus les diviseurs réciproques de la formule $t^2+cu^2$, lorsque $N$ et $c$ sont divisibles par un même facteur quarré. On sait déjà, par le n°. 192, combien de fois le nombre $N$ est contenu dans les diviseurs quadratiques de la formule $t^2+cu^2$; mais dans le cas dont il s'agit, ces diviseurs peuvent être de la première ou de la troisième espèce, et la difficulté est de distinguer dans le résultat les combinaisons qui appartiennent à la première espèce seulement. Voici une règle qui remplit cet objet dans uu grand nombre de cas.

| | |
|---|---|
| Pour chaque nombre premier, simple ou élevé à une puissance, qui divise $N$ sans diviser $c$, mettez............... | 2 |
| Pour chaque facteur simple $\alpha$ commun entre $N$ et $c$.... | 1 |
| Pour chaque facteur double $\alpha^2$ commun entre $N$ et $c$... | $\frac{1}{2}(\alpha-1)$ |
| Pour chaque facteur triple $\alpha^3$ commun entre $N$ et $c$.... | $\alpha$ |
| Pour chaque facteur quadruple $\alpha^4$, commun entre $N$ et $c$ | $\frac{1}{2}\alpha(\alpha-1)$ |
| Ainsi de suite; et si un nombre premier $\alpha$ divise plusieurs fois $N$ et $c$, mais ne les divise pas un même nombre de fois, mettez à raison du facteur excédent....... | 2 |

Multipliez eusuite tous ces nombres entr'eux, et prenez la moitié du produit, vous aurez le uombre de manières dout $N$ est conteuu dans les diviseurs réciproques de $t^2+cu^2$.

Soit par exemple $N=9225=3^2.5^2.41$, $c=189=3^3.3.7$, le nombre de fois que $N$ est compris dans les diviseurs réciproques de $t^2+cu^2$, sera, suivant cette règle, $\frac{1}{2}.\frac{3-1}{2}.2.2.2=4$. En effet si ou représente par $9225y^2+2qyz+rz^2$ le diviseur de $t^2+189u^2$, dans lequel 9225 est contenu, on trouvera, conformément au n°. 192, six valeurs de $q$ moindres que $\frac{1}{2}N$ et telles que $\frac{q^2+c}{N}=$ un entier $=r$. Ces six valeurs donuent six formes pour le diviseur quadratique $9225y^2+2qyz+rz^2$; mais en supprimant celles qui ne sont pas relatives à la première espèce, il ne reste que les quatre suivantes :

$$9225y^2+1812yz+98z^2$$
$$9225y^2+7962yz+1727z^2$$
$$9225y^2+3288yz+293z^2$$
$$9225y^2+9012yz+2201z^2,$$

ce qui s'accorde avec la règle précédente.

De même si on a $N=3^4.11.17$, $c=3^4.2$, on trouve par cette règle que $c$ est contenu $\frac{1}{2}.3.\frac{3-1}{2}$ ou $1\frac{1}{2}$ fois dans les diviseurs quadratiques de la formule $t^2+Nu^2$; et il faut observer que la fraction $\frac{1}{2}$ est l'indice d'un diviseur quadratique dont deux coefficiens sont égaux. On trouve en effet, dans ce cas, les deux diviseurs quadratiques $162y^2+54yz+98z^2$, $162y^2+162yz+134z^2$, où l'on voit que le second est compté pour $\frac{1}{2}$, parce qu'il ne répond qu'à deux formes trinaires de $N$, tandis que l'autre en comprend quatre (Voy. n°. 279).

La règle précédente à laquelle il faudra apporter quelques modifications pour la rendre absolument générale, indique assez que la circonstance du facteur quarré, commun entre $N$ et $c$, ne fait qu'augmenter dans une même proportion le nombre des formes trinaires correspondantes de $N$ et de $c$, de sorte que l'on trouvera toujours $2^{i-1}$ pour le nombre des formes trinaires de chacun des diviseurs réciproques dans lesquels $c$ est contenu. Mais pour pouvoir tirer cette conclusion avec certitude, il faut prouver que dans tout diviseur réciproque de la formule $t^2+Nu^2$, il existe toujours un nombre $c$ qui ne tombe pas dans l'exception du Théorême X.

Pour cet effet, soit $fy^2+2gyz+hz^2$ le diviseur proposé réduit à son expression la plus simple, en sorte qu'on ait $2g<f$ et $h$, et $f<\sqrt{\frac{4}{3}N}$; si le nombre $f$ est $<\sqrt{N}$, l'équation $f^2=y^2+N$ sera impossible, et ainsi on pourra prendre $c=f$, ce qui est un premier cas très-étendu où le choix du nombre $c$ n'aura aucune difficulté.

Si on a $f>\sqrt{N}$, j'observe que les trois plus petits nombres compris dans le diviseur proposé $fy^2+2gyz+hz^2$, savoir $f$, $h$, $f-2g+h$, sont chacun plus petits que $2\sqrt{N}$. Car on a déjà $f<\sqrt{\frac{4}{3}N}$; on a en même temps $f>\sqrt{N}$ et $fh<\frac{4}{3}N$, ce qui donne $h<\frac{4}{3}\sqrt{N}$;

soit $f=(1+\alpha)\sqrt{N}$, $h=(1+\beta)\sqrt{N}$, on aura $g^2=fh-N=(\alpha+\beta+\alpha\beta)N$; donc $f-2g+h=[2+\alpha+\beta-2\sqrt{(\alpha+\beta+\alpha\beta)}]\sqrt{N}$. Mais on a $\alpha<-1+\sqrt{\frac{4}{3}}$, $\beta<\frac{1}{3}$, donc $2\sqrt{(\alpha+\beta+\alpha\beta)}$ est plus grand que $\alpha+\beta$; donc $f-2g+h$ est plus petit qne $2\sqrt{N}$.

Les trois nombres $f$, $h$, $f-2g+h$, étant chacun plus petits que $2\sqrt{N}$, si on appelle $c$ l'un d'entr'eux, et que l'équation $c^2=y^2+Nz^2$ soit possible, il faudra qu'on ait $z=1$, ou $c=y^2+N$. Cela posé, il y a différens cas à examiner selon les diverses formes du nombre $N$.

Soit 1°. $N$ double d'un impair, en sorte que la formule $t^2+Nu^2$ appartienne à l'une des Tables X ou XI, l'équation $c^2=y^2+N$ sera impossible, parce que $c^2-y^2$ est toujours ou impair ou multiple de 4. Donc on pourra prendre pour $c$ celui qu'on voudra des trois nombres $f$, $h$, $f-2g+h$, et l'exception du Théorême X n'aura lieu pour aucun d'eux.

2°. Soit $N$ de la forme $4n+1$, en sorte que la formule $t^2+Nu^2$ se rapporte à la Table VIII, il est évident que des trois nombres $f, h, f-2g+h$, il y en aura au moins un pair. Or je remarque que si $c$ est pair, l'équation $c^2=y^2+N$, ne peut avoir lieu, parce que $c^2-y^2$ est de la forme $4n$, si $y$ est pair, ou de la forme $4n-1$ si $y$ est impair, de sorte que cette quantité n'est jamais de la même forme que $N$. Donc on pourra prendre pour $c$ le nombre pair ou l'un des nombres pairs qui se trouvent parmi les trois nombres $f$, $h$, $f-2g+h$.

3°. Enfin si le nombre $N$ est de forme $8n+3$, ou si le diviseur proposé appartient à la Table IX, il conviendra de mettre ce diviseur sous la forme $2fy^2+2gyz+2hz^2$, où l'on a à l'ordinaire $f, g, h$ impairs et $4fh-gg=N$. Dans ce diviseur, les trois nombres $2f$, $2h$, $2f-2g+2h$ seront toujours plus petits que $2\sqrt{N}$, mais on ne voit plus, comme dans les cas précédens, rien qui empêche qne ces trois nombres ne satisfassent, chacun en particulier, à l'équation $c^2=y^2+N$. Si cependant l'un d'entre eux a un commun diviseur avec $N$, on peut prouver que quand même l'équation $c^2=y^2+N$ seroit satisfaite, le nombre $c$ ne tombera pas dans l'exception du Théorême X.

En effet si les nombres $N$ et $c$ sont divisibles par un même nombre

premier $\pi$, et qu'on ait l'équation $c^2 = \theta^2 + N$, il faudra que $\theta$ soit aussi divisible par $\pi$; or on a, suivant le n°. 292,

$$c = \alpha^2 + \beta^2 + \gamma^2$$
$$b = \alpha\alpha' + \beta\beta' + \gamma\gamma'$$
$$c = \alpha'^2 + \beta'^2 + \gamma'^2.$$

Ces trois quantités étant divisibles chacune par $\pi$, on en conclura que la quantité $\gamma'^2 c - 2\gamma\gamma' b + \gamma^2 c$, ou son égale

$$(\alpha'\gamma - \alpha\gamma')^2 + (\beta'\gamma - \beta\gamma')^2$$

est divisible par $\pi$. On trouvera semblablement que les deux quantités

$$(\alpha'\beta - \alpha\beta')^2 + (\alpha'\gamma - \alpha\gamma')^2$$
$$(\alpha'\beta - \alpha\beta')^2 + (\beta'\gamma - \beta\gamma')^2$$

sont divisibles par $\pi$. Donc il faut que chacun des nombres $\alpha'\beta - \alpha\beta'$, $\alpha'\gamma - \alpha\gamma'$, $\beta'\gamma - \beta\gamma'$, soit divisible par $\pi$. Mais d'après l'analyse du n°. 292, ces trois mêmes nombres ont pour commun diviseur $\varphi$, et au moyen de ce commun diviseur on doit avoir $c^2 = \theta^2 + N\varphi^2$; donc puisque dans le cas que nous considérons on a $c^2 = \theta^2 + N$, il faudra que $\varphi$, et par conséquent $\pi$, soit égal à l'unité; donc l'exception du Théorème X n'aura pas lieu, si $c$ et $N$ ont un commun diviseur, quand même on auroit $c^2 = \theta^2 + N$; donc alors toutes les formes trinaires de $N$, considéré comme diviseur de $t^2 + cu^2$, seront différentes entr'elles; d'où il suit que le nombre $c$ pourra être employé à la démonstration du Théorême XVI.

On voit maintenant que si le diviseur proposé est de la forme $2fy^2 + 2gyz + 2fz^2$, auquel cas on a $N = 4f^2 - g^2$, le nombre $4f - 2g$ peut être pris pour $c$, parce que sa moitié $2f - g$ est diviseur de $N$. De même si le diviseur proposé est de la forme $2fy^2 + 2gyz + 2gz^2$, auquel cas on a $N = 4fg - g^2$, le nombre $2g$ peut être pris pour $c$, puisque $g$ est diviseur de $N$. Ces cas généraux sont ceux où le quarré du diviseur proposé pourra être réduit à la forme $y^2 + Nz^2$; car on trouvera aisément (n°. 367)

$$(2fy^2 + 2gyz + 2fz^2)^2 = (gy^2 + 2fyz + gz^2)^2 + N(y^2 - z^2)^2$$
$$(2fy^2 + 2gyz + 2gz^2)^2 = (\overline{g - 2f}.y^2 + 2gyz + 2gz^2)^2 + N(y^2 + 2yz)^2;$$

et il suit de ces formules, que tout nombre compris dans l'une ou dans l'autre, a son quarré de la forme $t^2+Nu^2$; il faut seulement en excepter les deux cas particuliers qui font évanouir le coefficient de $N$. Ces cas sont dans la première, $y=1$, $z=1$, et $y=1$, $z=-1$; d'où résultent les valeurs exceptées $c=4f+2g$, $c=4f-2g$, dont les moitiés sont diviseurs de $N$. Dans la seconde, les cas exceptés sont pareillement, $y=0$, $z=1$ et $y=2$, $z=-1$, d'où résultent $c=2g$, $c=8f-4g$, dont les moitiés sont encore diviseurs de $N$. On voit donc que le résultat de ces formules s'accorde parfaitement avec l'analyse précédente et celle du Théorème X; c'est ce qu'on peut vérifier sur le diviseur $38y^2+22yz+38z^2$, où l'on trouve deux nombres propres à être pris pour $c$, savoir $38-22+38$ ou $54$, et $38+22+38$ ou $98$. Ce dernier satisfait à l'équation $c^2=y^2+N$, mais il a un commun diviseur avec $N$.

Pour revenir à notre troisième Cas, où le diviseur proposé relatif à la Table IX est $2fy^2+2gyz+2hz^2$, si l'un des trois nombres $2f$, $2h$, $2f-2g+2h$, pris pour $c$, ne satisfait pas à l'équation $c^2=y^2+N$, ou si l'un d'eux a un commun diviseur avec $N$, ce nombre sera celui que l'on cherche, et toutes les valeurs trinaires de $N$ considéré comme diviseur de $t^2+cu^2$, seront différentes entr'elles. Le nombre dont il s'agit se trouve immédiatement lorsque le diviseur proposé a deux coefficiens égaux, c'est-à-dire, lorsque son quarré est de la forme $y^2+Nz^2$; et cette remarque ajoute le complément qui manquoit à la démonstration du Cas II (n°. 314). Lorsque $f$, $g$, $h$ seront inégaux, il est bien peu probable qu'on ait à-la-fois les trois équations $4f^2=y^2+N$, $4h^2=y'^2+N$, $(2f-2g+2h)^2=y''^2+N$, ou que du moins l'un des nombres $2f$, $2h$, $2f-2g+2h$, n'ait pas un diviseur commun avec $N$. Si cependant toutes ces conditions se trouvoient réunies, il faudroit chercher parmi tous les nombres moindres que $N$, compris dans le diviseur $2fy^2+2gyz+2hz^2$, un nombre $c$ qui ne satisfît pas à l'équation $c^2=y^2+Nz^2$. On en peut trouver d'autant plus facilement, que si tous les nombres compris dans le diviseur $2fy^2+2gyz+2hz^2$ devoient satisfaire à l'équation $c^2=y^2+Nz^2$, il faudroit que ce diviseur eût deux coefficiens égaux, et qu'il retombât ainsi dans le cas déjà résolu.

Il n'y a donc plus rien à desirer sur cette théorie, si ce n'est la démonstration de la règle générale mentionnée ci-dessus, ou d'une règle analogue qui serve à trouver combien de fois un nombre $N$, qui a un diviseur quarré commun avec $c$, est compris dans les diviseurs réciproques de la formule $t^2 + cu^2$; il suffit même de prouver que le facteur quarré, commun entre $N$ et $c$, augmente le nombre des combinaisons dans un rapport égal, soit qu'on considère $N$ comme diviseur de $t^2 + cu^2$, ou $c$ comme diviseur de $t^2 + Nu^2$. Or la question réduite à cet état ne semble plus présenter de grandes difficultés.

---

# TABLE I.

Expressions les plus simples des formules $L\,y^2 + 2\,M\,y\,z + N\,z^2$, pour toutes les valeurs du nombre non quarré $A = M^2 - L\,N$ depuis $A = 2$ jusqu'à $A = 136$.

| NOMBRE $A$. | FORMULE RÉDUITE. |
|---|---|
| 2 | $y^2 - 2z^2$ |
| 3 | $\pm(y^2 - 3z^2)$ |
| 5 | $y^2 - 5z^2$ |
| 6 | $\pm(y^2 - 6z^2)$ |
| 7 | $\pm(y^2 - 7z^2)$ |
| 8 | $\pm(y^2 - 8z^2)$ |
| 10 | $y^2 - 10z^2$<br>$2y^2 - 5z^2$ |
| 11 | $\pm(y^2 - 11z^2)$ |
| 12 | $\pm(y^2 - 12z^2)$ |
| 13 | $y^2 - 13z^2$ |
| 14 | $\pm(y^2 - 14z^2)$ |
| 15 | $\pm(y^2 - 15z^2)$<br>$\pm(3y^2 - 5z^2)$ |
| 17 | $y^2 - 17z^2$ |
| 18 | $\pm(y^2 - 18z^2)$ |
| 19 | $\pm(y^2 - 19z^2)$ |
| 20 | $\pm(y^2 - 20z^2)$ |
| 21 | $\pm(y^2 - 21z^2)$ |
| 22 | $\pm(y^2 - 22z^2)$ |
| 23 | $\pm(y^2 - 23z^2)$ |
| 24 | $\pm(y^2 - 24z^2)$<br>$\pm(3y^2 - 8z^2)$ |
| 26 | $y^2 - 26z^2$<br>$2y^2 - 13z^2$ |
| 27 | $\pm(y^2 - 27z^2)$ |
| 28 | $\pm(y^2 - 28z^2)$ |
| 29 | $y^2 - 29z^2$ |
| 30 | $\pm(y^2 - 30z^2)$<br>$\pm(2y^2 - 15z^2)$ |
| 31 | $\pm(y^2 - 31z^2)$ |
| 32 | $\pm(y^2 - 32z^2)$ |
| 33 | $\pm(y^2 - 33z^2)$ |
| 34 | $\pm(y^2 - 34z^2)$<br>$\pm(3y^2 + 2yz - 11z^2)$ |
| 35 | $\pm(y^2 - 35z^2)$<br>$\pm(5y^2 - 7z^2)$ |
| 37 | $y^2 - 37z^2$<br>$3y^2 + 2yz - 12z^2$ |
| 38 | $\pm(y^2 - 38z^2)$ |
| 39 | $\pm(y^2 - 39z^2)$<br>$\pm(2y^2 + 2yz - 19z^2)$ |
| 40 | $\pm(y^2 - 40z^2)$<br>$\pm(5y^2 - 8z^2)$ |
| 41 | $y^2 - 41z^2$ |
| 42 | $\pm(y^2 - 42z^2)$<br>$\pm(2y^2 - 21z^2)$ |
| 43 | $\pm(y^2 - 43z^2)$ |
| 44 | $\pm(y^2 - 44z^2)$ |
| 45 | $\pm(y^2 - 45z^2)$ |
| 46 | $\pm(y^2 - 46z^2)$ |
| 47 | $\pm(y^2 - 47z^2)$ |
| 48 | $\pm(y^2 - 48z^2)$<br>$\pm(3y^2 - 16z^2)$ |
| 50 | $y^2 - 50z^2$<br>$2y^2 - 25z^2$ |
| 51 | $\pm(y^2 - 51z^2)$<br>$\pm(3y^2 - 17z^2)$ |

TABLE I.

| NOMBRE $A$. | FORMULE RÉDUITE. |
|---|---|
| 52 | $\pm(y^2 - 52z^2)$ |
| 53 | $y^2 - 53z^2$ |
| 54 | $\pm(y^2 - 54z^2)$ |
| 55 | $\pm(y^2 - 55z^2)$<br>$\pm(2y^2 + 2yz - 27z^2)$ |
| 56 | $\pm(y^2 - 56z^2)$<br>$\pm(5y^2 + 2yz - 11z^2)$ |
| 57 | $\pm(y^2 - 57z^2)$ |
| 58 | $y^2 - 58z^2$<br>$2y^2 - 29z^2$ |
| 59 | $\pm(y^2 - 59z^2)$ |
| 60 | $\pm(y^2 - 60z^2)$<br>$\pm(3y^2 - 20z^2)$ |
| 61 | $y^2 - 61z^2$ |
| 62 | $\pm(y^2 - 62z^2)$ |
| 63 | $\pm(y^2 - 63z^2)$<br>$\pm(7y^2 - 9z^2)$ |
| 65 | $y^2 - 65z^2$<br>$5y^2 - 13z^2$ |
| 66 | $\pm(y^2 - 66z^2)$<br>$\pm(3y^2 - 22z^2)$ |
| 67 | $\pm(y^2 - 67z^2)$ |
| 68 | $\pm(y^2 - 68z^2)$ |
| 69 | $\pm(y^2 - 69z^2)$ |
| 70 | $\pm(y^2 - 70z^2)$<br>$\pm(2y^2 - 35z^2)$ |
| 71 | $\pm(y^2 - 71z^2)$ |
| 72 | $\pm(y^2 - 72z^2)$<br>$\pm(4y^2 + 4yz - 17z^2)$ |
| 73 | $y^2 - 73z^2$ |
| 74 | $y^2 - 74z^2$<br>$2y^2 - 37z^2$ |

| NOMBRE $A$. | FORMULE RÉDUITE. |
|---|---|
| 75 | $\pm(y^2 - 75z^2)$<br>$\pm(3y^2 - 25z^2)$ |
| 76 | $\pm(y^2 - 76z^2)$ |
| 77 | $\pm(y^2 - 77z^2)$ |
| 78 | $\pm(y^2 - 78z^2)$<br>$\pm(2y^2 - 39z^2)$ |
| 79 | $\pm(y^2 - 79z^2)$<br>$\pm(3y^2 + 2yz - 26z^2)$ |
| 80 | $\pm(y^2 - 80z^2)$<br>$\pm(5y^2 - 16z^2)$ |
| 82 | $y^2 - 82z^2$<br>$2y^2 - 41z^2$<br>$3y^2 + 2yz - 27z^2$ |
| 83 | $\pm(y^2 - 83z^2)$ |
| 84 | $\pm(y^2 - 84z^2)$<br>$\pm(7y^2 - 12z^2)$ |
| 85 | $y^2 - 85z^2$<br>$3y^2 + 2yz - 28z^2$ |
| 86 | $\pm(y^2 - 86z^2)$ |
| 87 | $\pm(y^2 - 87z^2)$<br>$\pm(3y^2 - 29z^2)$ |
| 88 | $\pm(y^2 - 88z^2)$<br>$\pm(8y^2 - 11z^2)$ |
| 89 | $y^2 - 89z^2$ |
| 90 | $\pm(y^2 - 90z^2)$<br>$\pm(2y^2 - 45z^2)$ |
| 91 | $\pm(y^2 - 91z^2)$<br>$\pm(7y^2 - 13z^2)$ |
| 92 | $\pm(y^2 - 92z^2)$ |
| 93 | $\pm(y^2 - 93z^2)$ |
| 94 | $\pm(y^2 - 94z^2)$ |

TABLE I.

| NOMBRE *A*. | FORMULE RÉDUITE. |
|---|---|
| 95 | $\pm(y^2 - 95z^2)$<br>$\pm(2y^2 + 2yz - 47z^2)$ |
| 96 | $\pm(y^2 - 96z^2)$<br>$\pm(3y^2 - 32z^2)$ |
| 97<br>98 | $y^2 - 97z^2$<br>$\pm(y^2 - 98z^2)$ |
| 99 | $\pm(y^2 - 99z^2)$<br>$\pm(9y^2 - 11z^2)$<br>$\pm(7y^2 + 2yz - 14z^2)$ |
| 101 | $y^2 - 101z^2$<br>$4y^2 + 2yz - 25z^2$ |
| 102 | $\pm(y^2 - 102z^2)$<br>$\pm(3y^2 - 34z^2)$ |
| 103 | $\pm(y^2 - 103z^2)$ |
| 104 | $\pm(y^2 - 104z^2)$<br>$\pm(8y^2 - 13z^2)$ |
| 105 | $\pm(y^2 - 105z^2)$<br>$\pm(3y^2 - 35z^2)$ |
| 106 | $y^2 - 106z^2$<br>$2y^2 - 53z^2$ |
| 107<br>108<br>109 | $\pm(y^2 - 107z^2)$<br>$\pm(y^2 - 108z^2)$<br>$y^2 - 109z^2$ |
| 110 | $\pm(y^2 - 110z^2)$<br>$\pm(2y^2 - 55z^2)$ |
| 111 | $\pm(y^2 - 111z^2)$<br>$\pm(2y^2 + 2yz - 55z^2)$ |
| 112 | $\pm(y^2 - 112z^2)$<br>$\pm(3y^2 + 2yz - 37z^2)$ |
| 113 | $y^2 - 113z^2$ |
| 114 | $\pm(y^2 - 114z^2)$<br>$\pm(3y^2 - 38z^2)$ |
| 115 | $\pm(y^2 - 115z^2)$<br>$\pm(5y^2 - 23z^2)$ |
| 116<br>117<br>118 | $\pm(y^2 - 116z^2)$<br>$\pm(y^2 - 117z^2)$<br>$\pm(y^2 - 118z^2)$ |
| 119 | $\pm(y^2 - 119z^2)$<br>$\pm(7y^2 - 17z^2)$ |
| 120 | $\pm(y^2 - 120z^2)$<br>$\pm(3y^2 - 40z^2)$<br>$\pm(5y^2 - 24z^2)$<br>$\pm(15y^2 - 8z^2)$ |
| 122 | $y^2 - 122z^2$<br>$2y^2 - 61z^2$ |
| 123 | $\pm(y^2 - 123z^2)$<br>$\pm(3y^2 - 41z^2)$ |
| 124<br>125 | $\pm(y^2 - 124z^2)$<br>$y^2 - 125z^2$ |
| 126 | $\pm(y^2 - 126z^2)$<br>$\pm(2y^2 - 63z^2)$ |
| 127<br>128<br>129 | $\pm(y^2 - 127z^2)$<br>$\pm(y^2 - 128z^2)$<br>$\pm(y^2 - 129z^2)$ |
| 130 | $y^2 - 130z^2$<br>$2y^2 - 65z^2$<br>$5y^2 - 26z^2$<br>$10y^2 - 13z^2$ |
| 131<br>132<br>133<br>134 | $\pm(y^2 - 131z^2)$<br>$\pm(y^2 - 132z^2)$<br>$\pm(y^2 - 133z^2)$<br>$\pm(y^2 - 134z^2)$ |
| 135 | $\pm(y^2 - 135z^2)$<br>$\pm(5y^2 - 27z^2)$ |
| 136 | $\pm(y^2 - 136z^2)$<br>$\pm(8y^2 - 17z^2)$<br>$\pm(3y^2 + 2yz - 45z^2)$ |

# TABLE II.

EXPRESSIONS les plus simples des formules $Ly^2 + Myz + Nz^2$, où $M$ est impair, pour toutes les valeurs de $B = M^2 - 4LN$ depuis $B = 5$ jusqu'à $B = 305$.

| NOMBRE $B$. | FORMULE RÉDUITE. |
|---|---|
| 5 | $y^2 + yz - z^2$ |
| 13 | $y^2 + yz - 3z^2$ |
| 17 | $y^2 + yz - 4z^2$ |
| 21 | $\pm(y^2 + yz - 5z^2)$ |
| 29 | $y^2 + yz - 7z^2$ |
| 33 | $\pm(y^2 + yz - 8z^2)$ |
| 37 | $y^2 + yz - 9z^2$ |
| 41 | $y^2 + yz - 10z^2$ |
| 45 | $\pm(y^2 + yz - 11z^2)$ |
| 53 | $y^2 + yz - 13z^2$ |
| 57 | $\pm(y^2 + yz - 14z^2)$ |
| 61 | $y^2 + yz - 15z^2$ |
| 65 | $y^2 + yz - 16z^2$ |
| | $2y^2 + yz - 8z^2$ |
| 69 | $\pm(y^2 + yz - 17z^2)$ |
| 73 | $y^2 + yz - 18z^2$ |
| 77 | $\pm(y^2 + yz - 19z^2)$ |
| 85 | $y^2 + yz - 21z^2$ |
| | $3y^2 + yz - 7z^2$ |
| 89 | $y^2 + yz - 22z^2$ |
| 93 | $\pm(y^2 + yz - 23z^2)$ |
| 97 | $y^2 + yz - 24z^2$ |
| 101 | $y^2 + yz - 25z^2$ |
| 105 | $\pm(y^2 + yz - 26z^2)$ |
| | $\pm(2y^2 + yz - 13z^2)$ |
| 109 | $y^2 + yz - 27z^2$ |
| 113 | $y^2 + yz - 28z^2$ |
| 117 | $\pm(y^2 + yz - 29z^2)$ |
| 125 | $y^2 + yz - 31z^2$ |
| 129 | $\pm(y^2 + yz - 32z^2)$ |
| 133 | $\pm(y^2 + yz - 33z^2)$ |
| 137 | $y^2 + yz - 34z^2$ |
| 141 | $\pm(y^2 + yz - 35z^2)$ |
| 145 | $y^2 + yz - 36z^2$ |
| | $2y^2 + yz - 18z^2$ |
| | $4y^2 + yz - 9z^2$ |
| 149 | $y^2 + yz - 37z^2$ |
| 153 | $\pm(y^2 + yz - 38z^2)$ |
| 157 | $\pm(y^2 + yz - 39z^2)$ |
| 161 | $\pm(y^2 + yz - 40z^2)$ |
| 165 | $\pm(y^2 + yz - 41z^2)$ |
| | $\pm(3y^2 + 3yz - 13z^2)$ |

| NOMBRE $B$. | FORMULE RÉDUITE. |
|---|---|
| 173 | $y^2 + yz - 43z^2$ |
| 177 | $\pm(y^2 + yz - 44z^2)$ |
| 181 | $y^2 + yz - 45z^2$ |
| 185 | $y^2 + yz - 46z^2$ |
| | $2y^2 + yz - 23z^2$ |
| 189 | $\pm(y^2 + yz - 47z^2)$ |
| 193 | $y^2 + yz - 48z^2$ |
| 197 | $y^2 + yz - 49z^2$ |
| 201 | $\pm(y^2 + yz - 50z^2)$ |
| 205 | $\pm(y^2 + yz - 51z^2)$ |
| | $\pm(3y^2 + yz - 17z^2)$ |
| 209 | $\pm(y^2 + yz - 52z^2)$ |
| 213 | $\pm(y^2 + yz - 53z^2)$ |
| 217 | $\pm(y^2 + yz - 54z^2)$ |
| 221 | $\pm(y^2 + yz - 55z^2)$ |
| | $\pm(5y^2 + yz - 11z^2)$ |
| 229 | $y^2 + yz - 57z^2$ |
| | $3y^2 + yz - 19z^2$ |
| 233 | $y^2 + yz - 58z^2$ |
| 237 | $\pm(y^2 + yz - 59z^2)$ |
| 241 | $y^2 + yz - 60z^2$ |
| 245 | $\pm(y^2 + yz - 61z^2)$ |
| 249 | $\pm(y^2 + yz - 62z^2)$ |
| 253 | $\pm(y^2 + yz - 63z^2)$ |
| 257 | $y^2 + yz - 64z^2$ |
| | $2y^2 + yz - 32z^2$ |
| 261 | $\pm(y^2 + yz - 65z^2)$ |
| 265 | $y^2 + yz - 66z^2$ |
| | $2y^2 + yz - 33z^2$ |
| 269 | $y^2 + yz - 67z^2$ |
| 273 | $\pm(y^2 + yz - 68z^2)$ |
| | $\pm(2y^2 + yz - 34z^2)$ |
| 277 | $y^2 + yz - 69z^2$ |
| 281 | $y^2 + yz - 70z^2$ |
| 285 | $\pm(y^2 + yz - 71z^2)$ |
| | $\pm(3y^2 + 3yz - 23z^2)$ |
| 293 | $y^2 + yz - 73z^2$ |
| 297 | $\pm(y^2 + yz - 74z^2)$ |
| 301 | $\pm(y^2 + yz - 75z^2)$ |
| 305 | $\pm(y^2 + yz - 76z^2)$ |
| | $\pm(2y^2 + yz - 38z^2)$ |

TABLE III.

# TABLE III.

DIVISEURS de la formule $t^2 - a u^2$.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
|---|---|---|
| $t^2 - 2u^2$ | $y^2 - 2z^2$ | $8x + 1, 7$ |
| $t^2 - 3u^2$ | $y^2 - 3z^2$<br>$3z^2 - y^2$ | $12x + 1$<br>$12x + 11$ |
| $t^2 - 5u^2$ | $y^2 - 5z^2$ | $20x + 1, 9, 11, 19$ |
| $t^2 - 6u^2$ | $y^2 - 6z^2$<br>$6z^2 - y^2$ | $24x + 1, 19$<br>$24x + 5, 23$ |
| $t^2 - 7u^2$ | $y^2 - 7z^2$<br>$7z^2 - y^2$ | $28x + 1, 9, 25$<br>$28x + 3, 19, 27$ |
| $t^2 - 10u^2$ | $y^2 - 10z^2$<br>$2y^2 - 5z^2$ | $40x + 1, 9, 31, 39$<br>$40x + 3, 13, 27, 37$ |
| $t^2 - 11u^2$ | $y^2 - 11z^2$<br>$11z^2 - y^2$ | $44x + 1, 5, 9, 25, 37$<br>$44x + 7, 19, 35, 39, 43$ |
| $t^2 - 13u^2$ | $y^2 - 13z^2$ | $52x + 1, 3, 9, 17, 23 : 25, 27, 29, 35, 43, 49, 51$ |
| $t^2 - 14u^2$ | $y^2 - 14z^2$<br>$14z^2 - y^2$ | $56x + 1, 9, 11, 25, 43, 51$<br>$56x + 5, 13, 31, 45, 47, 55$ |
| $t^2 - 15u^2$ | $y^2 - 15z^2$<br>$15z^2 - y^2$<br>$3y^2 - 5z^2$<br>$5z^2 - 3y^2$ | $60x + 1, 49$<br>$60x + 11, 59$<br>$60x + 7, 43$<br>$60x + 17, 53$ |
| $t^2 - 17u^2$ | $y^2 - 17z^2$ | $68x + 1, 9, 13, 15, 19 : 21, 25, 33, 35, 43 : 47, 49, 53, 55, 59 : 67$ |
| $t^2 - 19u^2$ | $y^2 - 19z^2$<br>$19z^2 - y^2$ | $76x + 1, 5, 9, 17, 25 : 45, 49, 61, 73$<br>$76x + 3, 15, 27, 31, 51 : 59, 67, 71, 75$ |
| $t^2 - 21u^2$ | $y^2 - 21z^2$<br>$21z^2 - y^2$ | $84x + 1, 25, 37, 43, 67, 79$<br>$84x + 5, 17, 41, 47, 59, 83$ |
| $t^2 - 22u^2$ | $y^2 - 22z^2$<br>$22z^2 - y^2$ | $88x + 1, 3, 9, 25, 27 : 49, 59, 67, 75, 81$<br>$88x + 7, 13, 21, 29, 39 : 61, 63, 79, 85, 87$ |
| $t^2 - 23u^2$ | $y^2 - 23z^2$<br>$23z^2 - y^2$ | $92x + 1, 9, 13, 25, 29 : 41, 49, 73, 77, 81 : 85$<br>$92x + 7, 11, 15, 19, 43 : 51, 63, 67, 79, 83 : 91$ |

# TABLE III.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
|---|---|---|
| $t^2 - 26u^2$ | $y^2 - 26z^2$<br>$2y^2 - 13z^2$ | $104x + 1, 9, 17, 23, 25 : 49, 55, 79, 81, 87 : 95, 103$<br>$104x + 5, 11, 19, 21, 37 : 45, 59, 67, 83, 85 : 93, 99$ |
| $t^2 - 29u^2$ | $y^2 - 29z^2$ | $116x + 1, 3, 5, 9, 13 : 23, 25, 33, 35, 45 : 49, 51, 53, 57, 59 : 63, 65, 67, 71, 81 : 83, 91, 93, 103, 107 : 109, 111, 115$ |
| $t^2 - 30u^2$ | $y^2 - 30z^2$<br>$30z^2 - y^2$<br>$2y^2 - 15z^2$<br>$15z^2 - 2y^2$ | $120x + 1, 19, 49, 91$<br>$120x + 29, 71, 101, 119$<br>$120x + 17, 83, 107, 113$<br>$120x + 7, 13, 37, 103$ |
| $t^2 - 31u^2$ | $y^2 - 31z^2$<br>$31z^2 - y^2$ | $124x + 1, 5, 9, 25, 33 : 41, 45, 49, 69, 81 : 97, 101, 109, 113, 121$<br>$124x + 3, 11, 15, 23, 27 : 43, 55, 75, 79, 83, 91, 99, 115, 119, 123$ |
| $t^2 - 33u^2$ | $y^2 - 33z^2$<br>$33z^2 - y^2$ | $132x + 1, 25, 31, 37, 49 : 67, 91, 97, 103, 115$<br>$132x + 17, 29, 35, 41, 65 : 83, 95, 101, 107, 131$ |
| $t^2 - 34u^2$ | $y^2 - 34z^2$<br>$34z^2 - y^2$<br>$3y^2 + 2yz - 11z^2$<br>$11z^2 - 2yz - 3y^2$ | $136x + 1, 9, 15, 25, 33 : 47, 49, 55, 81, 87 : 89, 103, 111, 121, 127 : 135$<br>$136x + 3, 5, 11, 27, 29 : 37, 45, 61, 75, 91 : 99, 107, 109, 125, 131 : 133$ |
| $t^2 - 35u^2$ | $y^2 - 35z^2$<br>$35z^2 - y^2$<br>$5y^2 - 7z^2$<br>$7z^2 - 5y^2$ | $140x + 1, 9, 29, 81, 109, 121$<br>$140x + 19, 31, 59, 111, 131, 139$<br>$140x + 13, 17, 33, 73, 97, 117$<br>$140x + 23, 43, 67, 107, 123, 127$ |
| $t^2 - 37u^2$ | $y^2 - 37z^2$<br>$3y^2 + 2yz - 12z^2$ | $148x + 1, 3, 7, 9, 11 : 21, 25, 27, 33, 41 : 47, 49, 53, 63, 65 : 67, 71, 73, 75, 77 : 81, 83, 85, 95, 99 : 101, 107, 115, 121, 123 : 127, 137, 139, 141, 145 : 147$ |
| $t^2 - 38u^2$ | $y^2 - 38z^2$<br>$38z^2 - y^2$ | $152x + 1, 9, 11, 17, 25 : 35, 43, 49, 73, 81 : 83, 99, 115, 121, 123 : 129, 137, 139$<br>$152x + 13, 15, 23, 29, 31 : 37, 53, 69, 71, 79 : 103, 109, 117, 127, 135 : 141, 143, 151$ |

## TABLE III.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
|---|---|---|
| $t^2 - 39u^2$ | $y^2 - 39z^2$<br>$39z^2 - y^2$<br>$2y^2 + 2yz - 19z^2$<br>$19z^2 - 2yz - 2y^2$ | $156x +$ 1, 25, 49, 61, 121, 133<br>$156x +$ 23, 35, 95, 107, 131, 155<br>$156x +$ 5, 41, 89, 125, 137, 149<br>$156x +$ 7, 19, 31, 67, 115, 151 |
| $t^2 - 41u^2$ | $y^2 - 41z^2$ | $164x +$ 1, 5, 9 21, 23 : 25, 31, 33, 37, 39 : 43, 45, 49, 51, 57 : 59, 61, 73, 77, 81 : 83, 87, 91, 103, 105 : 107, 113, 115, 119, 121 : 125, 127, 131, 133, 139 : 141, 143, 155, 159, 163 |
| $t^2 - 42u^2$ | $y^2 - 42z^2$<br>$42z^2 - y^2$<br>$2y^2 - 21z^2$<br>$21z^2 - 2y^2$ | $168x +$ 1, 25, 79, 121, 127, 151<br>$168x +$ 17, 41, 47, 89, 143, 167<br>$168x +$ 11, 29, 53, 107, 149, 155<br>$168x +$ 13, 19, 61, 115, 139, 157 |
| $t^2 - 43u^2$ | $y^2 - 43z^2$<br>$43z^2 - y^2$ | $172x +$ 1, 9, 13, 17, 21 : 25, 41, 49, 53, 57 : 81, 97, 101, 109, 117 : 121, 133, 145, 153, 165 : 169<br>$172x +$ 3, 7, 19, 27, 39 : 51, 55, 63, 71, 75 : 91, 115, 119, 123, 131 : 147, 151, 155, 159, 163 : 171 |
| $t^2 - 46u^2$ | $y^2 - 46z^2$<br>$46z^2 - y^2$ | $184x +$ 1, 3, 9, 25, 27 : 35, 41, 49, 59, 73 : 75, 81, 105, 121, 123 : 131, 139, 147, 163, 169 : 177, 179<br>$184x +$ 5, 7, 15, 21, 37 : 45, 53, 61, 63, 79 : 103, 109, 111, 125, 135 : 143, 149, 157, 159, 175, 181, 183 |
| $t^2 - 47u^2$ | $y^2 - 47z^2$<br>$47z^2 - y^2$ | $188x +$ 1, 9, 17, 21, 25 : 37, 49, 53, 61, 65 : 81, 89, 97, 101, 121 : 145, 149, 153, 157, 165 : 169, 173, 177<br>$188x +$ 11, 15, 19, 23, 31 : 35, 39, 43, 67, 87 : 91, 99, 107, 123, 127 : 135, 139, 151, 163, 167 : 171, 179, 187 |
| $t^2 - 51u^2$ | $y^2 - 51z^2$<br>$51z^2 - y^2$<br>$3y^2 - 17z^2$<br>$17z^2 - 3y^2$ | $204x +$ 1, 13, 25, 49, 121, 145, 157, 169<br>$204x +$ 35, 47, 59, 83, 155, 179, 191, 203<br>$204x +$ 7, 31, 79, 91, 139, 163, 175, 199<br>$204x +$ 5, 29, 41, 65, 113, 125, 173, 197 |

# TABLE III.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
|---|---|---|
| $t^2 - 53 u^2$ | $y^2 - 53 z^2$ | $212 x + 1, 7, 9, 11, 13 : 15, 17, 25, 29, 37 : 43, 47, 49, 57, 59 : 63, 69, 77, 81, 89 : 91, 93, 95, 97, 99 : 105, 107, 113, 115, 117 : 119, 121, 123, 131, 135 : 143, 149, 153, 155, 163 : 165, 169, 175, 183, 187 : 195, 197, 199, 201, 203 : 205, 211$ |
| $t^2 - 55 u^2$ | $y^2 - 55 z^2$ | $220 x + 1, 9, 49, 69, 81 : 89, 141, 169, 181, 201$ |
| | $55 z^2 - y^2$ | $220 x + 19, 39, 51, 79, 131 : 139, 151, 171, 211, 219$ |
| | $2 y^2 + 2 y z - 27 z^2$ | $220 x + 13, 17, 57, 73, 117 : 153, 173, 193, 197, 217$ |
| | $27 z^2 - 2 y z - 2 y^2$ | $220 x + 3, 23, 27, 47, 67 : 103, 147, 163, 203, 207$ |
| $t^2 - 57 u^2$ | $y^2 - 57 z^2$ | $228 x + 1, 7, 25, 43, 49 : 55, 61, 73, 85, 115 : 121, 139, 157, 163, 169 : 175, 187, 199$ |
| | $57 z^2 - y^2$ | $228 x + 29, 41, 53, 59, 65 : 71, 89, 107, 113, 143 : 155, 167, 173, 179, 185 : 203, 221, 227$ |
| $t^2 - 58 u^2$ | $y^2 - 58 z^2$ | $232 x + 1, 7, 9, 23, 25 : 33, 49, 57, 63, 65 : 71, 81, 103, 111, 121 : 129, 151, 161, 167, 169 : 175, 183, 199, 207, 209 : 223, 225, 231$ |
| | $2 y^2 - 29 z^2$ | $232 x + 3, 11, 19, 21, 27 : 37, 43, 61, 69, 75 : 77, 85, 99, 101, 131 : 133, 147, 155, 157, 163 : 171, 189, 195, 205, 211 : 213, 221, 229$ |
| $t^2 - 59 z^2$ | $y^2 - 59 z^2$ | $236 x + 1, 5, 9, 17, 21 : 25, 29, 41, 45, 49 : 53, 57, 81, 85, 105 : 121, 125, 133, 137, 145 : 153, 169, 181, 189, 193 : 197, 205, 213, 225$ |
| | $59 z^2 - y^2$ | $236 x + 11, 23, 31, 39, 43 : 47, 55, 67, 83, 91 : 99, 103, 111, 115, 131 : 151, 155, 179, 183, 187 : 191, 195, 207, 211, 215 : 219, 227, 231, 235$ |

## TABLE III.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
|---|---|---|
| $t^2 - 61u^2$ | $y^2 - 61z^2$ | $244x +$ 1, 5, 7, 9, 11 : 13, 23, 25, 31, 35 : 41, 43, 45, 49, 51 : 55, 57, 59, 63, 65 : 67, 71, 73, 77, 79 : 81, 87, 91, 97, 99 : 109, 111, 113, 115, 117 : 121, 125, 137, 139, 141 : 143, 149, 151, 155, 159 : 161, 169, 175, 191, 197 : 205, 207, 211, 215, 217 : 223, 225, 227, 229, 241 |
| $t^2 - 62u^2$ | $y^2 - 62z^2$ | $248x +$ 1, 9, 19, 25, 33 : 35, 41, 49, 51, 59 : 67, 81, 97, 103, 113 : 121, 129, 131, 163, 169 : 171, 187, 193, 195, 211 : 219, 225, 227, 233, 235 |
| | $62z^2 - y^2$ | $248x +$ 13, 15, 21, 23, 29 : 37, 53, 55, 61, 77 : 79, 85, 117, 119, 127 : 135, 141, 151, 167, 181 : 189, 197, 199, 207, 213 : 215, 223, 229, 239, 247 |
| $t^2 - 65u^2$ | $y^2 - 65z^2$ | $260x +$ 1, 9, 29, 49, 51 : 61, 69, 79, 81, 101 : 121, 129, 131, 139, 159 : 179, 181, 191, 199, 209 : 211, 231, 251, 259 |
| | $5y^2 - 13z^2$ | $260x +$ 7, 33, 37, 47, 57 : 63, 67, 73, 83, 93 : 97, 123, 137, 163, 167 : 177, 187, 193, 197, 203 : 213, 223, 227, 253 |
| $t^2 - 66u^2$ | $y^2 - 66z^2$ | $264x +$ 1, 25, 31, 49, 97 : 103, 169, 199, 223, 247 |
| | $66z^2 - y^2$ | $264x +$ 17, 41, 65, 95, 161 : 167, 215, 233, 239, 263 |
| | $3y^2 - 22z^2$ | $264x +$ 5, 53, 59, 125, 155 : 179, 203, 221, 245, 251 |
| | $22z^2 - 3y^2$ | $264x +$ 13, 19, 43, 61, 85 : 109, 139, 205, 211, 259 |
| $t^2 - 67u^2$ | $y^2 - 67z^2$ | $268x +$ 1, 9, 17, 21, 25 : 29, 33, 37, 49, 65 : 73, 77, 81, 89, 93 : 121, 129, 149, 153, 157 : 169, 173, 181, 189, 193 : 205, 217, 225, 237, 241 : 257, 261, 265 |
| | $67z^2 - y^2$ | $268x +$ 3, 7, 11, 27, 31 : 43, 51, 63, 75, 79 : 87, 95, 99, 111, 115 : 119, 139, 147, 175, 179 : 187, 191, 195, 203, 219 : 231, 235, 239, 243, 247 : 251, 259, 267 |

## TABLE III.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
|---|---|---|
| $t^2 - 69u^2$ | $y^2 - 69z^2$ | $276x + 1, 13, 25, 31, 49 : 55, 73, 85, 121, 127 : 133, 139, 151, 163, 169 : 187, 193, 211, 223, 259 : 265, 271$ |
| | $69z^2 - y^2$ | $276x + 5, 11, 17, 53, 65 : 83, 89, 107, 113, 125 : 137, 143, 149, 155, 191 : 203, 221, 227, 245, 251 : 263, 275$ |
| $t^2 - 70u^2$ | $y^2 - 70z^2$ | $280x + 1, 9, 11, 51, 81 : 99, 121, 169, 179, 211 : 219, 249$ |
| | $70z^2 - y^2$ | $280x + 31, 61, 69, 101, 111 : 159, 181, 199, 229, 269 : 271, 279$ |
| | $2y^2 - 35z^2$ | $280x + 23, 37, 53, 93, 127 : 183, 197, 207, 247, 253 : 263, 277$ |
| | $35z^2 - 2y^2$ | $280x + 3, 17, 27, 33, 73 : 83, 97, 153, 187, 227 : 243, 257$ |
| $t^2 - 71u^2$ | $y^2 - 71z^2$ | $284x + 1, 5, 9, 25, 29 : 37, 45, 49, 57, 73 : 77, 81, 89, 101, 109 : 121, 125, 129, 145, 157 : 161, 169, 185, 217, 221 : 225, 229, 233, 237, 245 : 249, 253, 261, 273, 277$ |
| | $71z^2 - y^2$ | $284x + 7, 11, 23, 31, 35 : 39, 47, 51, 55, 59 : 63, 67, 99, 115, 123 : 127, 139, 155, 159, 163 : 175, 183, 195, 203, 207 : 211, 227, 235, 239, 247 : 255, 259, 275, 279, 283$ |
| $t^2 - 73u^2$ | $y^2 - 73z^2$ | $292x + 1, 3, 9, 19, 23 : 25, 27, 35, 37, 41 : 49, 55, 57, 61, 65 : 67, 69, 71, 75, 77 : 79, 81, 85, 89, 91 : 97, 105, 109, 111, 119 : 121, 123, 127, 137, 143 : 145, 147, 149, 155, 165 : 169, 171, 173, 181, 183 : 187, 195, 201, 203, 207 : 211, 213, 215, 217, 221 : 223, 225, 227, 231, 235 : 237, 243, 251, 255, 257 : 265, 267, 269, 273, 283 : 289, 291$ |

## TABLE III.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
|---|---|---|
| $t^2 - 74u^2$ | $y^2 - 74z^2$ | $296x + 1, 7, 9, 25, 33 : 41, 47, 49, 63, 65 : 71, 73, 81, 95, 121 : 127, 137, 145, 151, 159 : 169, 175, 201, 215, 223 : 225, 231, 233, 247, 249 : 255, 263, 271, 287, 289 : 295$ |
| | $2y^2 - 37z^2$ | $296x + 5, 13, 19, 29, 35 : 43, 45, 51, 59, 61 : 69, 91, 93, 109, 117 : 125, 131, 133, 163, 165 : 171, 179, 187, 203, 205 : 227, 235, 237, 245, 251 : 253, 261, 267, 277, 283 : 291$ |
| $t^2 - 77u^2$ | $y^2 - 77z^2$ | $308x + 1, 9, 15, 23, 25 : 37, 53, 67, 71, 81 : 93, 113, 135, 141, 155 : 163, 169, 177, 179, 191 : 207, 221, 225, 235, 247 : 255, 267, 289, 291, 295$ |
| | $77z^2 - y^2$ | $308x + 13, 17, 19, 41, 53 : 61, 73, 83, 87, 101 : 117, 129, 131, 139, 145 : 153, 167, 173, 195, 215 : 227, 237, 241, 255, 271 : 283, 285, 293, 299, 307$ |
| $t^2 - 78u^2$ | $y^2 - 78z^2$ | $312x + 1, 25, 43, 49, 121 : 139, 211, 217, 235, 259 : 283, 289$ |
| | $78z^2 - y^2$ | $312x + 23, 29, 53, 77, 95 : 101, 173, 191, 263, 269 : 287, 311$ |
| | $2y^2 - 39z^2$ | $312x + 11, 41, 59, 83, 89 : 137, 161, 203, 227, 275 : 281, 305$ |
| | $39z^2 - y^2$ | $312x + 7, 31, 37, 85, 109 : 151, 175, 223, 229, 253 : 271, 301$ |
| $t^2 - 79u^2$ | $y^2 - 79z^2$<br>$26y^2 + 2yz - 3z^2$ | $316x + 1, 5, 9, 13, 21 : 25, 45, 49, 65, 73 : 81, 89, 97, 101, 105 : 117, 121, 125, 129, 141 : 169, 177, 181, 189, 209 : 213, 225, 241, 245, 253 : 257, 269, 273, 277, 281 : 289, 301, 309, 313$ |
| | $79z^2 - y^2$<br>$3z^2 - 2yz - 26y^2$ | $316x + 3, 7, 15, 27, 35 : 39, 43, 47, 59, 63 : 71, 75, 91, 103, 107 : 127, 135, 139, 147, 175 : 187, 191, 195, 199, 211, 215, 219, 227, 235, 243 : 251, 267, 271, 291, 295 : 303, 307, 311, 315$ |

# TABLE IV.

DIVISEURS de la formule $t^2+au^2$, $a$ étant un nombre de la forme $4n+1$.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
|---|---|---|
| $t^2+u^2$ | $y^2+z^2$ | $4x+1$ |
| $t^2+5u^2$ | $y^2+2yz+6z^2$<br>$2y^2+2yz+3z^2$ | $20x+1, 9$<br>$20x+3, 7$ |
| $t^2+13u^2$ | $y^2+2yz+14z^2$<br>$2y^2+2yz+7z^2$ | $52x+1, 9, 17, 25, 29 : 49$<br>$52x+7, 11, 15, 19, 31 : 47$ |
| $t^2+17u^2$ | $y^2+2yz+18z^2$<br>$2y^2+2yz+9z^2$<br>$3y^2+2yz+6z^2$ | $68x+1, 9, 13, 21, 25 : 33, 49, 53$ (for the first two)<br>$68x+3, 7, 11, 23, 27 : 31, 39, 63$ |
| $t^2+21u^2$ | $y^2+2yz+22z^2$<br>$2y^2+2yz+11z^2$<br>$5y^2+6yz+6z^2$<br>$10y^2+6yz+3z^2$ | $84x+1, 25, 37$<br>$84x+11, 23, 71$<br>$84x+5, 17, 41$<br>$84x+19, 31, 55$ |
| $t^2+29u^2$ | $y^2+2yz+30z^2$<br>$5y^2+2yz+6z^2$<br>$2y^2+2yz+15z^2$<br>$10y^2+2yz+3z^2$ | $116x+1, 5, 9, 13, 25 : 33, 45, 49, 53, 57 : 65, 81, 93, 109$<br>$116x+3, 11, 15, 19, 27 : 31, 39, 43, 47, 55 : 75, 79, 95, 99$ |
| $t^2+33u^2$ | $y^2+2yz+34z^2$<br>$2y^2+2yz+17z^2$<br>$3y^2+6yz+14z^2$<br>$6y^2+6yz+7z^2$ | $132x+1, 25, 37, 49, 97$<br>$132x+17, 29, 41, 65, 101$<br>$132x+23, 47, 59, 71, 119$<br>$132x+7, 19, 43, 79, 127$ |
| $t^2+37u^2$ | $y^2+2yz+38z^2$<br>$2y^2+2yz+19z^2$ | $148x+1, 9, 21, 25, 33 : 41, 49, 53, 65, 73 : 77, 81, 85, 101, 121 : 137, 141, 145$<br>$148x+15, 19, 23, 31, 35 : 39, 43, 51, 55, 59 : 79, 87, 91, 103, 119 : 131, 135, 143$ |
| $t^2+41u^2$ | $y^2+2yz+42z^2$<br>$2y^2+2yz+21z^2$<br>$5y^2+6yz+10z^2$<br>$3y^2+2yz+14z^2$<br>$6y^2+2yz+7z^2$ | $164x+1, 5, 9, 21, 25 : 33, 37, 45, 49, 57 : 61, 73, 77, 81, 105 : 113, 121, 125, 133, 141$ (for the first three)<br>$164x+3, 7, 11, 15, 19 : 27, 35, 47, 55, 63 : 67, 71, 75, 79, 95 : 99, 111, 135, 147, 151$ (for the last two) |

*NOTA.* Les diviseurs quadratiques contiennent, outre les diviseurs impairs mentionnés dans la table, des diviseurs pairs ; savoir, les diviseurs $8n+2$ lorsque $a$ est de forme $8m+1$, et les diviseurs $8n+6$ lorsque $a$ est de forme $8m+5$.

TABLE IV.

## TABLE IV.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
|---|---|---|
| $t^2+53u^2$ | $y^2+2yz+54z^2$<br>$9y^2+2yz+6z^2$ | $212x+$ 1, 9, 13, 17, 25 : 29, 37, 49, 57, 69 : 77, 81, 89, 93, 97 : 105, 113, 117, 121, 149 : 153, 165, 169, 197, 201 : 205 |
| | $2y^2+2yz+27z^2$<br>$18y^2+2yz+3z^2$ | $212x+$ 3, 19, 23, 27, 31 : 35, 39, 51, 55, 67 : 71, 75, 79, 83, 87 : 103, 111, 127, 139, 147 : 151, 167, 171, 179, 191 : 207 |
| $t^2+57u^2$ | $y^2+2yz+58z^2$ | $228x+$ 1, 25, 49, 61, 73 : 85, 121, 157, 169 |
| | $2y^2+2yz+29z^2$ | $228x+$ 29, 41, 53, 65, 89 : 113, 173, 185, 221 |
| | $3y^2+6yz+22z^2$ | $228x+$ 31, 67, 79, 91, 103 : 127, 151, 211, 223 |
| | $6y^2+6yz+11z^2$ | $228x+$ 11, 23, 35, 47, 83 : 119, 131, 191, 215 |
| $t^2+61u^2$ | $y^2+2yz+62z^2$<br>$5y^2+6yz+14z^2$ | $244x+$ 1, 5, 9, 13, 25 : 41, 45, 49, 57, 65 : 73, 77, 81, 97, 109 : 113, 117, 121, 125, 137 : 141, 149, 161, 169, 197 : 205, 217, 225, 229, 241 |
| | $2y^2+2yz+31z^2$<br>$10y^2+6yz+7z^2$ | $244x+$ 7, 11, 23, 31, 35 : 43, 51, 55, 59, 63 : 67, 71, 79, 87, 91 : 99, 111, 115, 139, 143 : 151, 155, 159, 175, 191 : 207, 211, 215, 223, 227 |
| $t^2+65u^2$ | $y^2+2yz+66z^2$<br>$9y^2+10yz+10z^2$ | $260x+$ 1, 9, 29, 49, 61 : 69, 81, 101, 121, 129 : 181, 209 |
| | $2y^2+2yz+33z^2$<br>$18y^2+10yz+5z^2$ | $260x+$ 33, 37, 57, 73, 93 : 97, 137, 177, 193, 197 : 213, 253 |
| | $3y^2+2yz+22z^2$ | $260x+$ 3, 23, 27, 43, 87 : 103, 107, 127, 147, 183 : 207, 243 |
| | $6y^2+2yz+11z^2$ | $260x+$ 11, 19, 31, 59, 71 : 99, 111, 119, 151, 171 : 219, 239 |
| $t^2+69u^2$ | $y^2+2yz+70z^2$<br>$13y^2+6yz+6z^2$ | $276x+$ 1, 13, 25, 49, 73 : 85, 121, 133, 169, 193 : 265 |
| | $5y^2+2yz+14z^2$ | $276x+$ 5, 17, 53, 65, 89 : 113, 125, 137, 149, 221 : 245 |
| | $2y^2+2yz+35z^2$<br>$26y^2+6yz+3z^2$ | $276x+$ 35, 47, 59, 71, 95 : 119, 131, 167, 179, 215 : 239 |
| | $10y^2+2yz+7z^2$ | $276x+$ 7, 19, 43, 67, 79 : 91, 103, 175, 199, 235 : 247 |

## TABLE IV.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
|---|---|---|
| $t^2 + 73u^2$ | $y^2 + 2yz + 74z^2$<br>$2y^2 + 2yz + 37z^2$ | $292x +$ 1, 9, 25, 37, 41 : 49, 57, 61, 65, 69 : 77, 81, 85, 89, 97 : 105, 109, 121, 137, 145 : 149, 165, 169, 173, 181 : 201, 213, 217, 221, 225 : 237, 257, 265, 269, 273 : 289 |
| | $7y^2 + 10yz + 14z^2$ | $292x +$ 7, 11, 15, 31, 39 : 43, 47, 51, 59, 63 : 83, 87, 95, 99, 103 : 107, 115, 131, 135, 139 : 151, 159, 163, 167, 175 : 179, 191, 199, 239, 247 : 259, 263, 271, 275, 279 : 287 |
| $t^2 + 77u^2$ | $y^2 + 2yz + 78z^2$<br>$9y^2 + 14yz + 14z^2$ | $308x +$ 1, 9, 25, 37, 53 : 81, 93, 113, 137, 141 : 169, 177, 221, 225, 289 |
| | $13y^2 + 2yz + 6z^2$ | $308x +$ 13, 17, 41, 73, 89 : 113, 117, 129, 145, 149 : 173, 241, 257, 285, 293 |
| | $2y^2 + 2yz + 39z^2$<br>$18y^2 + 14yz + 7z^2$ | $308x +$ 39, 43, 51, 79, 95 : 107, 123, 127, 151, 183 : 211, 219, 239, 263, 303 |
| | $26y^2 + 2yz + 3z^2$ | $308x +$ 3, 27, 31, 47, 59 : 75, 103, 111, 115, 159 : 199, 223, 243, 251, 279 |
| $t^2 + 85u^2$ | $y^2 + 2yz + 86z^2$ | $340x +$ 1, 9, 21, 49, 69 : 81, 89, 101, 121, 149 : 161, 169, 189, 229, 281 : 321 |
| | $5y^2 + 10yz + 22z^2$ | $340x +$ 37, 57, 73, 97, 113 : 133, 173, 177, 193, 197 : 233, 277, 313, 317, 333, 337 |
| | $2y^2 + 2yz + 43z^2$ | $340x +$ 43, 47, 67, 83, 87 : 103, 123, 127, 183, 203 : 223, 247, 263, 287, 307 : 327 |
| | $10y^2 + 10yz + 11z^2$ | $340x +$ 11, 31, 39, 71, 79 : 91, 99, 131, 139, 159 : 199, 211, 231, 279, 299 : 311 |
| $t^2 + 89u^2$ | $y^2 + 2yz + 90z^2$<br>$2y^2 + 2yz + 45z^2$<br>$5y^2 + 2yz + 18z^2$<br>$10y^2 + 2yz + 9z^2$ | $356x +$ 1, 5, 9, 17, 21 : 25, 45, 49, 53, 57 : 69, 73, 81, 85, 93 : 97, 105, 109, 121, 125 : 129, 133, 153, 157, 161 : 169, 173, 177, 189, 217 : 225, 233, 245, 249, 257 : 265, 269, 277, 285, 289 : 301, 309, 317, 345 |
| | $3y^2 + 2yz + 30z^2$<br>$6y^2 + 2yz + 15z^2$<br>$7y^2 + 6yz + 14z^2$ | $356x +$ 3, 7, 15, 19, 23 : 27, 31, 35, 43, 51 : 59, 63, 75, 83, 95 : 103, 115, 119. 127, 135 : 143, 147, 151, 155, 159 : 163, 171, 175, 191, 207 : 211, 215, 219, 239, 243 : 255, 279, 291, 295, 315 : 319, 323, 327, 343 |



# TABLE IV.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
| --- | --- | --- |
| $t^2 + 93u^2$ | $y^2 + 2yz + 94z^2$ | $372x + 1, 25, 49, 97, 109 : 121, 133, 157, 169, 193 : 205, 253, 289, 349, 361$ |
| | $17y^2 + 6yz + 6z^2$ | $372x + 17, 29, 53, 65, 77 : 89, 137, 161, 185, 197 : 209, 269, 305, 353, 365$ |
| | $2y^2 + 2yz + 47z^2$ | $372x + 35, 47, 59, 71, 95 : 107, 131, 143, 191, 227 : 287, 299, 311, 335, 359$ |
| | $34y^2 + 6yz + 3z^2$ | $372x + 43, 55, 79, 91, 115 : 127, 139, 151, 199, 223 : 247, 259, 271, 331, 367$ |
| $t^2 + 97u^2$ | $y^2 + 2yz + 98z^2$<br>$2y^2 + 2yz + 49z^2$ | $388x + 1, 9, 25, 33, 49 : 53, 61, 65, 73, 81 : 85, 89, 93, 101, 105 : 109, 113, 121, 129, 133 : 141, 145, 161, 169, 185 : 193, 197, 205, 221, 225 : 229, 237, 241, 269, 273 : 285, 289, 293, 297, 309 : 313, 341, 345, 353, 357 : 361, 377, 385$ |
| | $7y^2 + 2yz + 14z^2$ | $388x + 7, 15, 19, 23, 39 : 51, 55, 59, 63, 67 : 71, 83, 87, 107, 111 : 123, 127, 131, 135, 139 : 143, 155, 171, 175, 179 : 187, 199, 207, 211, 215 : 223, 231, 235, 239, 251 : 263, 271, 311, 319, 331 : 343, 347, 351, 359, 367 : 371, 375, 383$ |
| $t^2 + 101u^2$ | $y^2 + 2yz + 102z^2$<br>$5y^2 + 6yz + 22z^2$<br>$17y^2 + 2yz + 6z^2$<br>$9y^2 + 10yz + 14z^2$ | $404x + 1, 5, 9, 13, 17 : 21, 25, 33, 37, 45 : 49, 65, 77, 81, 85 : 97, 105, 117, 121, 125 : 137, 153, 157, 165, 169 : 177, 181, 185, 189, 193 : 197, 201, 221, 225, 233 : 245, 249, 273, 281, 289 : 297, 305, 313, 321, 329 : 357, 361, 373, 381, 385$ |
| | $2y^2 + 2yz + 51z^2$<br>$10y^2 + 6yz + 11z^2$<br>$34y^2 + 2yz + 3z^2$<br>$18y^2 + 10yz + 7z^2$ | $404x + 3, 7, 11, 15, 27 : 35, 39, 51, 55, 59 : 63, 67, 75, 83, 91 : 99, 103, 111, 119, 127 : 135, 139, 143, 147, 151 : 163, 167, 175, 187, 191 : 195, 199, 231, 243, 255 : 259, 263, 271, 275, 291 : 295, 311, 315, 331, 335 : 343, 347, 351, 363, 375$ |
| $t^2 + 105u^2$ | $y^2 + 2yz + 106z^2$ | $420x + 1, 109, 121, 169, 289, 361$ |
| | $2y^2 + 2yz + 53z^2$ | $420x + 53, 113, 137, 197, 233, 317$ |
| | $10y^2 + 10yz + 13z^2$ | $420x + 13, 73, 97, 157, 313, 397$ |
| | $5y^2 + 10yz + 26z^2$ | $420x + 41, 89, 101, 209, 269, 341$ |
| | $3y^2 + 6yz + 38z^2$ | $420x + 47, 83, 143, 167, 227, 383$ |
| | $6y^2 + 6yz + 19z^2$ | $420x + 19, 31, 139, 199, 271, 391$ |
| | $7y^2 + 14yz + 22z^2$ | $420x + 43, 67, 127, 163, 247, 403$ |
| | $14y^2 + 14yz + 11z^2$ | $420x + 11, 71, 179, 191, 239, 359$ |

# TABLE V.

Diviseurs de la formule $t^2 + a u^2$, $a$ étant un nombre de la forme $4n-1$.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
|---|---|---|
| $t^2+3u^2$ | $y^2+yz+z^2$ | $6x+1$ |
| $t^2+7u^2$ | $y^2+7z^2$ | $14x+1, 9, 11$ |
| $t^2+11u^2$ | $y^2+yz+3z^2$ | $22x+1, 3, 5, 9, 15$ |
| $t^2+15u^2$ | $y^2+15z^2$<br>$3y^2+5z^2$ | $30x+1, 19$<br>$30x+17, 23$ |
| $t^2+19u^2$ | $y^2+yz+5z^2$ | $38x+1, 5, 7, 9, 11 : 17, 23, 25, 35$ |
| $t^2+23u^2$ | $y^2+23z^2$<br>$3y^2+2yz+8z^2$ | $46x+1, 3, 9, 13, 25 : 27, 29, 31, 35, 39 : 41$ |
| $t^2+31u^2$ | $y^2+31z^2$<br>$5y^2+4yz+7z^2$ | $62x+1, 5, 7, 9, 19 : 25, 33, 35, 39, 41 : 45, 47, 49, 51, 59$ |
| $t^2+35u^2$ | $y^2+yz+9z^2$<br>$3y^2+yz+3z^2$ | $70x+1, 9, 11, 29, 39, 51$<br>$70x+3, 13, 17, 27, 33, 47$ |
| $t^2+39u^2$ | $y^2+39z^2$<br>$3y^2+13z^2$<br>$5y^2+2yz+8z^2$ | $78x+1, 25, 43, 49, 55, 61$<br>$78x+5, 11, 41, 47, 59, 71$ |
| $t^2+43u^2$ | $y^2+yz+11z^2$ | $86x+1, 9, 11, 13, 15 : 17, 21, 23, 25, 31 : 35, 41, 47, 49, 53 : 57, 59, 67, 79, 81 : 83$ |
| $t^2+47u^2$ | $y^2+47z^2$<br>$3y^2+2yz+16z^2$<br>$7y^2+6yz+8z^2$ | $94x+1, 3, 7, 9, 17 : 21, 25, 27, 37, 49 : 51, 53, 55, 59, 61 : 63, 65, 71, 75, 79 : 81, 83, 89$ |
| $t^2+51u^2$ | $y^2+yz+13z^2$<br>$3y^2+3yz+5z^2$ | $102x+1, 13, 19, 25, 43 : 49, 55, 67$<br>$102x+5, 11, 23, 29, 41 : 65, 71, 95$ |
| $t^2+55u^2$ | $y^2+55z^2$<br>$5y^2+11z^2$<br>$7y^2+2yz+8z^2$ | $110x+1, 9, 31, 49, 59 : 69, 71, 81, 89, 91$<br>$110x+7, 13, 17, 43, 57 : 63, 73, 83, 87, 107$ |
| $t^2+59u^2$ | $y^2+yz+15z^2$<br>$3y^2+yz+5z^2$ | $118x+1, 3, 5, 7, 9 : 15, 17, 19, 21, 25 : 27, 29, 35, 41, 45 : 49, 51, 53, 57, 63 : 71, 75, 79, 81, 85 : 87, 95, 105, 107$ |

# TABLE V.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
|---|---|---|
| $t^2 + 67u^2$ | $y^2 + yz + 17z^2$ | $134x +$ 1, 9, 15, 17, 19 : 21, 23, 25, 29, 33 : 35, 37, 39, 47, 49 : 55, 59, 65, 71, 73 : 77, 81, 83, 89, 91 : 93, 103, 107, 121, 123 : 127, 129, 131 |
| $t^2 + 71u^2$ | $y^2 + 71z^2$<br>$3y^2 + 2yz + 24z^2$<br>$9y^2 + 2yz + 8z^2$<br>$5y^2 + 4yz + 15z^2$ | $142x +$ 1, 3, 5, 9, 15 : 19, 25, 27, 29, 37 : 43, 45, 49, 57, 73 : 75, 77, 79, 81, 83 : 87, 89, 91, 95, 101 : 103, 107, 109, 111, 119 : 121, 125, 129, 131, 135 |
| $t^2 + 79u^2$ | $y^2 + 79z^2$<br>$5y^2 + 2yz + 16z^2$<br>$11y^2 + 6yz + 8z^2$ | $158x +$ 1, 5, 9, 11, 13 : 19, 21, 23, 25, 31 : 45, 49, 51, 55, 65 : 67, 73, 81, 83, 87 : 89, 95, 97, 99, 101 : 105, 111, 115, 117, 119 : 121, 123, 125, 129, 131 : 141, 143, 151, 155 |
| $t^2 + 83u^2$ | $y^2 + yz + 21z^2$<br>$3y^2 + yz + 7z^2$ | $166x +$ 1, 3, 7, 9, 11 : 17, 21, 23, 25, 27 : 29, 31, 33, 37, 41 : 49, 51, 59, 61, 63 : 65, 69, 75, 77, 81 : 87, 93, 95, 99, 109 : 111, 113, 119, 121, 123 : 127, 131, 147, 151, 153 : 161 |
| $t^2 + 87u^2$ | $y^2 + 87z^2$<br>$7y^2 + 4yz + 13z^2$<br>$3y^2 + 29z^2$<br>$11y^2 + 2yz + 8z^2$ | $174x +$ 1, 7, 13, 25, 49 : 67, 91, 103, 109, 115 : 121, 139, 151, 169<br>$174x +$ 11, 17, 41, 47, 77 : 89, 95, 101, 113, 119 : 131, 137, 143, 155 |
| $t^2 + 91u^2$ | $y^2 + yz + 23z^2$<br><br>$5y^2 + 3yz + 5z^2$ | $182x +$ 1, 9, 23, 25, 29 : 43, 51, 53, 79, 81 : 95, 107, 113, 121, 127 : 155, 165, 179<br>$182x +$ 5, 7, 19, 31, 33 : 41, 45, 47, 59, 73 : 83, 89, 97, 111, 125 : 145, 167, 171 |
| $t^2 + 95u^2$ | $y^2 + 95z^2$<br>$5y^2 + 19z^2$<br>$9y^2 + 4yz + 11z^2$<br>$3y^2 + 2yz + 32z^2$<br>$13y^2 + 6yz + 8z^2$ | $190x +$ 1, 9, 11, 39, 49 : 61, 81, 99, 101, 111 : 119, 121, 131, 139, 149 : 159, 161; 169<br>$190x +$ 3, 13, 27, 33, 37 : 53, 67, 97, 103, 107 : 113, 117, 127, 143, 147 : 167, 173, 183 |
| $t^2 + 103u^2$ | $y^2 + 103z^2$<br>$13y^2 + 2yz + 8z^2$<br>$7y^2 + 6yz + 16z^2$ | $206x +$ 1, 7, 9, 13, 15 : 17, 19, 23, 25, 29 : 33, 41, 49, 55, 59 : 61, 63, 79, 81, 83 : 91, 93, 97, 105, 107 : 111, 117, 119, 121, 129 : 131, 133, 135, 137, 139 : 141, 149, 153, 155, 159 : 161, 163, 167, 169, 171 : 175, 179, 185, 195, 201 : 203 |

# TABLE VI.

DIVISEURS de la formule $t^2+2au^2$, $a$ étant un nombre de la forme $4n+1$.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
|---|---|---|
| $t^2+2u^2$ | $y^2+2z^2$ | $8x+1, 3$ |
| $t^2+10u^2$ | $y^2+10z^2$<br>$2y^2+5z^2$ | $40x+1, 9, 11, 19$<br>$40x+7, 13, 23, 37$ |
| $t^2+26u^2$ | $y^2+26z^2$<br>$3y^2+4yz+10z^2$<br>$2y^2+13z^2$<br>$6y^2+4yz+5z^2$ | $104x+1, 3, 9, 17, 25 : 27, 35, 43, 49, 51, 75, 81$<br>$104x+5, 7, 15, 21, 31 : 37, 45, 47, 63, 71 : 85, 93$ |
| $t^2+34u^2$ | $y^2+34z^2$<br>$2y^2+17z^2$<br>$5y^2+8yz+10z^2$ | $136x+1, 9, 19, 25, 33 : 35, 43, 49, 59, 67 : 81, 83, 89, 115, 121 : 123$<br>$136x+5, 7, 23, 29, 31 : 37, 39, 45, 61, 63 : 71, 79, 95, 109, 125 : 133$ |
| $t^2+42u^2$ | $y^2+42z^2$<br>$3y^2+14z^2$<br>$6y^2+7z^2$<br>$2y^2+21z^2$ | $168x+1, 25, 43, 67, 121, 163$<br>$168x+17, 41, 59, 83, 89, 131$<br>$168x+13, 31, 55, 61, 103, 157$<br>$168x+23, 29, 53, 71, 95, 149$ |
| $t^2+58u^2$ | $y^2+58z^2$<br>$2y^2+29z^2$ | $232x+1, 9, 25, 33, 35 : 49, 51, 57, 59, 65 : 67, 81, 83, 91, 107 : 115, 121, 123, 129, 139 : 161, 169, 179, 187, 209 : 219, 225, 227$<br>$232x+15, 21, 31, 37, 39 : 47, 55, 61, 69, 77 : 79, 85, 95, 101, 119 : 127, 133, 135, 143, 157 : 159, 189, 191, 205, 213 : 215, 221, 229$ |
| $t^2+66u^2$ | $y^2+66z^2$<br>$3y^2+22z^2$<br>$2y^2+33z^2$<br>$6y^2+11z^2$<br>$5y^2+4yz+14z^2$<br>$10y^2+4yz+7z^2$ | $264x+1, 25, 49, 67, 91 : 97, 115, 163, 169, 235$<br>$264x+17, 35, 41, 65, 83 : 107, 131, 161, 227, 233$<br>$264x+5, 23, 47, 53, 71 : 119, 125, 191, 221, 245$<br>$264x+7, 13, 61, 79, 85 : 109, 127, 151, 175, 205$ |

## TABLE VI.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
| --- | --- | --- |
| $t^2+74u^2$ | $y^2+74z^2$<br>$3y^2+4yz+26z^2$<br>$9y^2+8yz+10z^2$ | $296x+1, 9, 11, 25, 27 : 33, 41, 49, 65, 67 : 73, 75, 81, 83, 99 : 107, 115, 121, 123, 137 : 139, 145, 147, 155, 169 : 195, 201, 211, 219, 225 : 233, 243, 249, 275, 289 : 299$ |
| | $2y^2+37z^2$<br>$6y^2+4yz+13z^2$<br>$18y^2+8yz+5z^2$ | $296x+5, 13, 15, 23, 29 : 31, 39, 45, 55, 61 : 69, 79, 87, 93, 103 : 109, 117, 119, 125, 133 : 135, 143, 165, 167, 183 : 191, 199, 205, 207, 237 : 239, 245, 253, 261, 277 : 279$ |
| $t^2+82u^2$ | $y^2+82z^2$<br>$2y^2+41z^2$ | $328x+1, 9, 25, 33, 43 : 49, 51, 57, 59, 73 : 81, 83, 91, 105, 107 : 113, 115, 121, 131, 139 : 155, 163, 169, 185, 187 : 195, 201, 203, 209, 225 : 241, 251, 267, 283, 289 : 291, 297, 305, 307, 323$ |
| | $7y^2+8yz+14z^2$ | $328x+7, 13, 15, 29, 47 : 53, 55, 63, 69, 71 : 79, 85, 93, 95, 101 : 109, 111, 117, 135, 149 : 151, 157, 167, 175, 181 : 183, 191, 199, 229, 231 : 239, 253, 261, 263, 293 : 301, 309, 311, 317, 325$ |
| $t^2+106u^2$ | $y^2+106z^2$<br>$11y^2+4yz+10z^2$ | $424x+1, 9, 11, 17, 25 : 43, 49, 57, 59, 81 : 89, 91, 97, 99, 105 : 107, 113, 115, 121, 123 : 131, 153, 155, 163, 169 : 187, 195, 201, 203, 211 : 219, 225, 227, 241, 249 : 259, 275, 281, 289, 305 : 307, 329, 331, 347, 355 : 361, 377, 387, 395, 409 : 411, 417$ |
| | $2y^2+53z^2$<br>$22y^2+4yz+5z^2$ | $424x+5, 21, 23, 31, 39 : 45, 55, 61, 71, 79 : 85, 87, 101, 103, 109 : 111, 125, 127, 133, 141 : 151, 157, 167, 173, 181 : 189, 191, 207, 215, 231 : 239, 245, 247, 253, 263 : 277, 279, 285, 287, 295 : 341, 349, 351, 357, 359 : 373, 383, 389, 391, 397 : 405, 421$ |

# TABLE VII.

DIVISEURS de la formule $t^2 + 2\,a u^2$, $a$ étant un nombre de la forme $4\,n - 1$.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
|---|---|---|
| $t^2 + 6u^2$ | $y^2+6z^2$<br>$2y^2+3z^2$ | $24x+1,\ 7$<br>$24x+5,\ 11$ |
| $t^2 + 14u^2$ | $y^2+14z^2$<br>$2y^2+7z^2$<br>$3y^2+4yz+6z^2$ | $56x+1,\ 9,\ 15,\ 23,\ 25,\ 39$<br>$56x+3,\ 5,\ 13,\ 19,\ 27,\ 45$ |
| $t^2 + 22u^2$ | $y^2+22z^2$<br>$2y^2+11z^2$ | $88x+1, 9, 15, 23, 25 : 31, 47, 49, 71, 81$<br>$88x+13, 19, 21, 29, 35 : 43, 51, 61, 83, 85$ |
| $t^2 + 30u^2$ | $y^2+30z^2$<br>$2y^2+15z^2$<br>$5y^2+6z^2$<br>$10y^2+3z^2$ | $120x+1,\ 31,\ 49,\ 79$<br>$120x+17, 23, 47, 113$<br>$120x+11, 29, 59, 101$<br>$120x+13,\ 37, 43, 67$ |
| $t^2 + 38u^2$ | $y^2+38z^2$<br>$6y^2+4yz+7z^2$<br>$2y^2+19z^2$<br>$3y^2+4yz+14z^2$ | $152x+1, 7, 9, 17, 23 : 25, 39, 47, 49, 55 :$<br>$63, 73, 81, 87, 111 : 119, 121, 137$<br>$152x+3, 13, 21, 27, 29 : 37, 51, 53, 59, 67 :$<br>$69, 75, 91, 107, 109 : 117, 141, 147$ |
| $t^2 + 46u^2$ | $y^2+46z^2$<br>$2y^2+23z^2$<br><br>$5y^2+4yz+10z^2$ | $184x+1, 9, 25, 31, 39 : 41, 47, 49, 55,$<br>$71 : 73, 81, 87, 95, 105 : 119, 121,$<br>$127, 151, 167 : 169, 177$<br>$184x+5, 11, 19, 21, 37 : 43, 45, 51, 53,$<br>$61 : 67, 83, 91, 99, 107 : 109, 125,$<br>$149, 155, 157 : 171, 181$ |
| $t^2 + 62u^2$ | $y^2+62z^2$<br>$2y^2+31z^2$<br>$7y^2+12yz+14z^2$<br><br>$6y^2+4yz+11z^2$<br>$3y^2+4yz+22z^2$ | $248x+1, 7, 9, 25, 33 : 39, 41, 47, 49,$<br>$63 : 71, 81, 87, 95, 97 : 103, 111,$<br>$113, 121, 129 : 143, 159, 169, 175,$<br>$183 : 191, 193, 225, 231, 233$<br>$248x+3, 11, 13, 21, 27 : 29, 37, 43, 53,$<br>$61 : 75, 77, 83, 85, 91 : 99, 115,$<br>$117, 123, 139 : 141, 147, 179, 181,$<br>$189 : 197, 203, 213, 229, 243$ |
| $t^2 + 70u^2$ | $y^2+70z^2$<br><br>$10y^2+7z^2$<br><br>$5y^2+14z^2$<br><br>$2y^2+35z^2$ | $280x+1, 9, 39, 71, 79 : 81, 121, 151,$<br>$169, 191 : 239, 249$<br>$280x+17, 33, 47, 73, 87 : 97, 103, 143,$<br>$153, 167 : 223, 257$<br>$280x+19, 59, 61, 69, 101 : 131, 139, 171,$<br>$181, 229 : 251, 269$<br>$280x+37, 43, 53, 67, 93 : 107, 123, 163,$<br>$197, 253 : 267, 277$ |

## TABLE VII.

| FORMULE. | DIVISEURS QUADRATIQUES. | DIVISEURS LINÉAIRES. |
|---|---|---|
| $t^2+78u^2$ | $y^2+78z^2$ | $312x+1, 25, 49, 55, 79 : 103, 121, 127, 199, 217 : 289, 295$ |
| | $2y^2+39z^2$ | $312x+41, 47, 71, 89, 119 : 137, 161, 167, 215, 239 : 281, 305$ |
| | $3y^2+26z^2$ | $312x+29, 35, 53, 77, 101 : 107, 131, 155, 173, 179 : 251, 269$ |
| | $6y^2+13z^2$ | $312x+19, 37, 67, 85, 109 : 115, 163, 187, 229, 253 : 301, 307$ |
| $t^2+86u^2$ | $y^2+86z^2$<br>$10y^2+4yz+9z^2$<br>$6y^2+4yz+15z^2$ | $344x+1, 9, 15, 17, 23 : 25, 31, 41, 47, 49 : 57, 79, 81, 87, 95 : 97, 103, 111, 121, 127 : 135, 143, 145, 153, 167 : 169, 183, 185, 193, 207 : 225, 231, 239, 255, 271 : 273, 279, 281, 289, 305 : 311, 337$ |
| | $2y^2+43z^2$<br>$5y^2+4yz+18z^2$<br>$3y^2+4yz+30z^2$ | $344x+3, 5, 19, 27, 29 : 37, 45, 51, 61, 69 : 75, 77, 85, 91, 93 : 115, 123, 125, 131, 141 : 147, 149, 155, 157, 163 : 171, 179, 205, 211, 227 : 235, 237, 243, 245, 261 : 277, 285, 291, 309, 323 : 331, 333$ |
| $t^2+94u^2$ | $y^2+94z^2$<br>$2y^2+47z^2$<br>$7y^2+4yz+14z^2$ | $376x+1, 7, 9, 17, 25 : 49, 55, 63, 65, 71 : 79, 81, 89, 95, 97 : 103, 111, 119, 121, 143 : 145, 153, 159, 169, 175 : 177, 183, 191, 209, 215 : 225, 239, 241, 247, 249 : 263, 271, 289, 303, 319 : 335, 337, 343, 345, 353 : 361$ |
| | $5y^2+8yz+22z^2$<br>$10y^2+8yz+11z^2$ | $376x+5, 11, 13, 19, 29 : 35, 43, 45, 67, 69 : 77, 85, 91, 93, 99 : 107, 109, 117, 123, 125 : 133, 139, 163, 171, 179 : 181, 187, 203, 211, 219 : 221, 227, 229, 245, 261 : 275, 293, 301, 315, 317 : 323, 325, 339, 349, 355 : 373$ |
| $t^2+102u^2$ | $y^2+102z^2$ | $408x+1, 25, 49, 55, 103 : 121, 127, 145, 151, 169 : 217, 223, 247, 271, 319 : 361$ |
| | $6y^2+17z^2$ | $408x+23, 41, 65, 71, 95 : 113, 143, 167, 209, 215 : 233, 311, 329, 335, 377 : 401$ |
| | $2y^2+51z^2$ | $408x+35, 53, 59, 77, 83 : 101, 149, 155, 179, 203 : 251, 293, 341, 365, 389 : 395$ |
| | $3y^2+34z^2$ | $408x+37, 61, 91, 109, 133 : 139, 163, 181, 211, 235 : 277, 283, 301, 379, 397 : 403$ |

# TABLE VIII.

DIVISEURS $4n+1$ de la formule $t^2+cu^2$, $c$ étant un nombre de la forme $4n+1$.

| NOMBRE $c$. | DIVISEURS $4n+1$. |
|---|---|
| | $\underbrace{t^2 + u^2}$ |
| 1 | $y^2+2yz+2z^2=(y+z)^2+z^2$ |
| | $\underbrace{t^2 + 5u^2}$ |
| 4+1 | $y^2+2yz+6z^2=(y+z)^2+z^2+4z^2$ |
| | $\underbrace{t^2 + 9u^2}$ |
| 4+4+1<br>9 | $2y^2+2yz+5z^2=\begin{cases} y^2+(y+z)^2+4z^2 \\ (y+2z)^2+(y-z)^2 \end{cases}$ |
| 9 | $y^2+2yz+10z^2=(y+z)^2+9z^2$ |
| | $\underbrace{t^2 + 13u^2}$ |
| 9+4 | $y^2+2yz+14z^2=(y+z)^2+4z^2+9z^2$ |
| | $\underbrace{t^2 + 17u^2}$ |
| 16+1<br>9+4+4 | $y^2+2yz+18z^2=(y+z)^2+z^2+16z^2$<br>$2y^2+2yz+9z^2=(y+2z)^2+(y-z)^2+4z^2$ |
| | $\underbrace{t^2 + 21u^2}$ |
| 16+4+1 | $5y^2+6yz+6z^2=\begin{cases} (2y+z)^2+(y+z)^2+4z^2 \\ (2y+2z)^2+(y-z)^2+z^2 \end{cases}$ |
| | $y^2+2yz+22z^2$ *non décomposable.* |
| | $\underbrace{t^2 + 25u^2}$ |
| 16+9<br>25 | $y^2+2yz+26z^2=\begin{cases} (y+z)^2+16z^2+9z^2 \\ (y+z)^2+25z^2 \end{cases}$ |
| 25<br>25 | $2y^2+2yz+13z^2=(y+3z)^2+(y-2z)^2$<br>$5y^2+10yz+10z^2=(2y+z)^2+(y+3z)^2$ |
| | $\underbrace{t^2 + 29u^2}$ |
| 25+4<br>16+9+4 | $y^2+2yz+30z^2=(y+z)^2+25z^2+4z^2$<br>$5y^2+2yz+6z^2=(y-z)^2+(2y+z)^2+4z^2$ |

## TABLE VIII.

| NOMBRE C. | DIVISEURS $4n+1$. |
|---|---|
| | $t^2+33u^2$ |
| 16+16+1<br>25+4+4 | $2y^2+2yz+17z^2=\begin{cases}y^2+(y+z)^2+16z^2\\(y+3z)^2+(y-2z)^2+4z^2\end{cases}$ |
| | $y^2+2yz+34z^2$ *non décomposable.* |
| | $t^2+37u^2$ |
| 36+1 | $y^2+2yz+38z^2=(y+z)^2+36z^2+z^2$ |
| | $t^2+41u^2$ |
| 25+16 | $y^2+2yz+42z^2=(y+z)^2+25z^2+16z^2$ |
| 16+16+9 | $2y^2+2yz+21z^2=(y+2z)^2+(y-z)^2+16z^2$ |
| 36+4+1 | $5y^2+6yz+10z^2=4y^2+(y+3z)^2+z^2$ |
| | $t^2+45u^2$ |
| 25+16+4<br>25+16+4<br>36+9 | $5y^2+10yz+14z^2=\begin{cases}(2y+3z)^2+(y-z)^2+4z^2\\(2y+z)^2+(y+3z)^2+4z^2\\(y+z)^2+(2y+2z)^2+9z^2\end{cases}$ |
| 36+9 | $9y^2+6yz+6z^2=(2y+2z)^2+(2y-z)^2+(y+z)^2$ |
| 36+9 | $y^2+2yz+46z^2=(y+z)^2+36z^2+9z^2$ |
| | $t^2+49u^2$ |
| 36+9+4<br>49 | $5y^2+2yz+10z^2=\begin{cases}4y^2+(y+z)^2+9z^2\\(y+3z)^2+(2y-z)^2\end{cases}$ |
| 49 | $y^2+2yz+50z^2=(y+z)^2+49z^2$ |
| 49 | $2y^2+2yz+25z^2=(y+4z)^2+(y-3z)^2$ |
| | $t^2+53u^2$ |
| 49+4 | $y^2+2yz+54z^2=(y+z)^2+49z^2+4z^2$ |
| 36+16+1 | $9y^2+2yz+6z^2=(2y-z)^2+(y-z)^2+(2y+2z)^2$ |
| | $t^2+57u^2$ |
| 49+4+4<br>25+16+16 | $2y^2+2yz+29z^2=\begin{cases}(y+4z)^2+(y-3z)^2+4z^2\\(y+3z)^2+(y-2z)^2+16z^2\end{cases}$ |
| | $y^2+2yz+58z^2$ *non décomposable.* |

# TABLE VIII.

| NOMBRE C. | DIVISEURS $4n+1$. |
|---|---|
| | $t^2+61u^2$ |
| 36+25 | $y^2+2yz+62z^2=(y+z)^2+36z^2+25z^2$ |
| 36+16+9 | $5y^2+6yz+14z^2=(2y+2z)^2+(y-z)^2+9z^2$ |
| | $t^2+65u^2$ |
| 64+1 | $y^2+2yz+66z^2=(y+z)^2+64z^2+z^2$ |
| 49+16 | $y^2+2yz+66z^2=(y+z)^2+49z^2+16z^2$ |
| 36+25+4 | $9y^2+10yz+10z^2=(2y+3z)^2+4y^2+(y-z)^2$ |
| | $9y^2+10yz+10z^2=(2y+z)^2+4y^2+(y+3z)^2$ |
| | $2y^2+2yz+33z^2$, $18y^2+10yz+5z^2$ *non décomposables.* |
| | $t^2+69u^2$ |
| 64+4+1 | $5y^2+2yz+14z^2=(2y+2z)^2+(y-3z)^2+z^2$ |
| 49+16+4 | $5y^2+2yz+14z^2=(2y-z)^2+(y+3z)^2+4z^2$ |
| | $y^2+2yz+70z^2$, $13y^2+6yz+6z^2$ *non décomposables.* |
| | $t^2+73u^2$ |
| 64+9 | $y^2+2yz+74z^2=(y+z)^2+64z^2+9z^2$ |
| 36+36+1 | $2y^2+2yz+37z^2=y^2+(y+z)^2+36z^2$ |
| | $t^2+77u^2$ |
| 36+25+16 | $13y^2+2yz+6z^2=(3y+z)^2+(2y-z)^2+4z^2$ |
| 64+9+4 | $13y^2+2yz+6z^2=(3y-z)^2+(2y+2z)^2+z^2$ |
| | $y^2+2yz+78z^2$, $9y^2+14yz+14z^2$ *non décomposables.* |
| | $t^2+81u^2$ |
| 49+16+16 | $2y^2+2yz+41z^2=(y+4z)^2+(y-3z)^2+16z^2$ |
| 36+36+9 | $2y^2+2yz+41z^2=(y+2z)^2+(y-z)^2+36z^2$ |
| 81 | $2y^2+2yz+41z^2=(y+5z)^2+(y-4z)^2$ |
| 64+16+1 | $5y^2+6yz+18z^2=(2y+z)^2+(y+z)^2+16z^2$ |
| 36+36+9 | $5y^2+6yz+18z^2=4y^2+(y+3z)^2+9z^2$ |
| 81 | $5y^2+6yz+18z^2=(2y+3z)^2+(y-3z)^2$ |
| 81 | $y^2+2yz+82z^2=(y+z)^2+81z^2$ |
| 81 | $9y^2+6yz+10z^2=(3y+z)^2+9z^2$ |
| 81 | $9y^2+18yz+18z^2=9(y+z)^2+9z^2$ |

# TABLE VIII.

| NOMBRE $c$. | DIVISEURS $4n+1$. |
|---|---|
| | $t^2+85u^2$. |
| 81+4 <br> 49+36 | $y^2+2yz+86z^2=\begin{cases}(y+z)^2+81z^2+4z^2\\(y+z)^2+49z^2+36z^2\end{cases}$ |
| | $5y^2+10yz+22z^2$ *non décomposable.* |
| | $t^2+89u^2$ |
| 64+25 | $y^2+2yz+90z^2=(y+z)^2+64z^2+25z^2$ |
| 81+4+4 | $2y^2+2yz+45z^2=(y+5z)^2+(y-4z)^2+4z^2$ |
| 64+16+9 | $5y^2+2yz+18z^2=(2y+z)^2+(y-z)^2+16z^2$ |
| 49+36+4 | $9y^2+2yz+10z^2=4y^2+(2y-z)^2+(y+3z)^2$ |
| | $t^2+93u^2$ |
| 64+25+4 | $17y^2+6yz+6z^2=\begin{cases}(4y+z)^2+(y-z)^2+4z^2\\(3y-z)^2+(2y+z)^2+(2y+2z)^2\end{cases}$ |
| | $y^2+2yz+94z^2$ *non décomposable.* |
| | $t^2+97u^2$ |
| 81+16 | $y^2+2yz+98z^2=(y+z)^2+81z^2+16z^2$ |
| 36+36+25 | $2y^2+2yz+49z^2=(y+3z)^2+(y-2z)^2+36z^2$ |
| | $t^2+101u^2$ |
| 100+1 | $y^2+2yz+102z^2=(y+z)^2+100z^2+z^2$ |
| 81+16+4 | $5y^2+6yz+22z^2=(2y+3z)^2+(y-3z)^2+4z^2$ |
| 64+36+1 | $17y^2+2yz+6z^2=(2y+z)^2+(3y+z)^2+(2y-2z)^2$ |
| 49+36+16 | $9y^2+10yz+14z^2=(y+3z)^2+(2y-z)^2+(2y+2z)^2$ |
| | $t^2+105u^2$ |
| 64+25+16 <br> 64+25+16 <br> 100+4+1 <br> 100+4+1 | $5y^2+10yz+26z^2=\begin{cases}(2y+z)^2+(y+3z)^2+16z^2\\(2y+3z)^2+(y-z)^2+16z^2\\(2y+4z)^2+(y-3z)^2+z^2\\4y^2+(y+5z)^2+z^2\end{cases}$ |
| | $\left.\begin{array}{l}y^2+2yz+106z^2\\2y^2+2yz+53z^2\\10y^2+10yz+13z^2\end{array}\right\}$ *non décomposables.* |
| | $t^2+109u^2$ |
| 100+9 | $y^2+2yz+110z^2=(y+z)^2+100z^2+9z^2$ |
| 64+36+9 | $5y^2+2yz+22z^2=(y-3z)^2+(2y+2z)^2+9z^2$ |

## TABLE VIII.

| NOMBRE *c*. | DIVISEURS $4n+1$. |
|---|---|
| | $t^2+113u^2$ |
| $64+49$ | $y^2+2yz+114z^2=(y+z)^2+64z^2+49z^2$ |
| $81+16+16$ | $2y^2+2yz+57z^2=(y+5z)^2+(y-4z)^2+16z^2$ |
| $100+9+4$ | $9y^2+14yz+18z^2=(2y+4z)^2+(2y-z)^2+(y+z)^2$ |
| | $t^2+117u^2$ |
| $100+16+1$<br>$64+49+4$<br>$81+36$ | $9y^2+6yz+14z^2=\begin{cases}(2y+3z)^2+(2y-2z)^2+(y+z)^2\\(2y+2z)^2+(2y+z)^2+(y-3z)^2\\(3y+z)^2+9z^2+4z^2\end{cases}$ |
| | $6y^2+6yz+21z^2$ *non décomposable.* |
| $81+36$ | $y^2+2yz+118z^2=(y+z)^2+81z^2+36z^2$ |
| $81+36$ | $9y^2+18yz+22z^2=9(y+z)^2+9z^2+4z^2$ |
| | $t^2+121u^2$ |
| $49+36+36$<br>$121$ | $2y^2+2yz+61z^2=\begin{cases}(y+4z)^2+(y-3z)^2+36z^2\\(y+6z)^2+(y-5z)^2\end{cases}$ |
| $81+36+4$<br>$121$ | $13y^2+6yz+10z^2=\begin{cases}(3y+z)^2+4y^2+9z^2\\(3y-z)^2+(2y+3z)^2\end{cases}$ |
| $121$ | $y^2+2yz+122z^2=(y+z)^2+121z^2$ |
| $121$ | $26y^2+6yz+5z^2=(5y+z)^2+(y+2z)^2$ |
| | $t^2+125u^2$ |
| $121+4$<br>$100+25$ | $y^2+2yz+126z^2=\begin{cases}(y+z)^2+121z^2+4z^2\\(y+z)^2+100z^2+25z^2\end{cases}$ |
| $64+36+25$<br>$100+25$ | $9y^2+2yz+14z^2=\begin{cases}(2y+z)^2+(2y-2z)^2+(y+3z)^2\\(2y+3z)^2+(2y-2z)^2+(y-z)^2\end{cases}$ |
| $100+16+9$<br>$100+25$ | $21y^2+2yz+6z^2=\begin{cases}(4y+z)^2+(y-z)^2+(2y-2z)^2\\(4y-z)^2+(y+z)^2+(2y+2z)^2\end{cases}$ |
| $100+25$ | $5y^2+10yz+30z^2=(y+z)^2+(2y+2z)^2+25z^2$ |
| | $t^2+129u^2$ |
| $64+64+1$<br>$121+4+4$ | $2y^2+2yz+65z^2=\begin{cases}y^2+(y+z)^2+64z^2\\(y+6z)^2+(y-5z)^2+4z^2\end{cases}$ |
| $100+25+4$<br>$64+49+16$ | $5y^2+2yz+26z^2=\begin{cases}4y^2+(y+z)^2+25z^2\\(2y-z)^2+(y+3z)^2+16z^2\end{cases}$ |
| | $\left.\begin{matrix}y^2+2yz+130z^2\\13y^2+2yz+10z^2\end{matrix}\right\}$ *non décomposables.* |

## TABLE VIII.

| NOMBRE $c$. | DIVISEURS $4n+1$. |
|---|---|
| | $\overbrace{t^2 + 133\,u^2}$ |
| 81+36+16 | $13y^2+14yz+14z^2=\begin{cases}(3y+3z)^2+(2y-z)^2+4z^2\\(3y+z)^2+(2y+2z)^2+9z^2\end{cases}$<br>$y^2+2yz+134z^2$ *non décomposable.* |
| | $\overbrace{t^2 + 137\,u^2}$ |
| 121+16<br>64+64+9<br>100+36+1 | $y^2+2yz+138z^2=(y+z)^2+121z^2+16z^2$<br>$2y^2+2yz+69z^2=(y+2z)^2+(y-z)^2+64z^2$<br>$9y^2+10yz+18z^2=(2y+4z)^2+(2y-z)^2+(y-z)^2$ |
| | $\overbrace{t^2 + 141\,u^2}$ |
| 121+16+4<br>100+25+16 | $5y^2+6yz+30z^2=\begin{cases}(2y-z)^2+(y+5z)^2+4z^2\\(2y+2z)^2+(y-z)^2+25z^2\end{cases}$<br>$\left.\begin{matrix}y^2+2yz+142z^2\\25y^2+6yz+6z^2\end{matrix}\right\}$ *non décomposables.* |
| | $\overbrace{t^2 + 145\,u^2}$ |
| 144+1<br>81+64 | $y^2+2yz+146z^2=\begin{cases}(y+z)^2+144z^2+z^2\\(y+z)^2+81z^2+64z^2\end{cases}$ |
| 100+36+9 | $5y^2+10yz+34z^2=\begin{cases}(y-3z)^2+(2y+4z)^2+9z^2\\(y+5z)^2+4y^2+9z^2\end{cases}$<br>$\left.\begin{matrix}2y^2+2yz+73z^2\\10y^2+10yz+17z^2\end{matrix}\right\}$ *non décomposables.* |
| | $\overbrace{t^2 + 149\,u^2}$ |
| 100+49<br>81+64+4<br>144+4+1<br>64+49+36 | $y^2+2yz+150z^2=(y+z)^2+100z^2+49z^2$<br>$9y^2+14yz+22z^2=(2y+2z)^2+(2y+3z)^2+(y-3z)^2$<br>$5y^2+2yz+30z^2=(y+5z)^2+(2y-2z)^2+z^2$<br>$25y^2+2yz+6z^2=(4y+z)^2+(3y-z)^2+4z^2$ |
| | $\overbrace{t^2 + 153\,u^2}$ |
| 64+64+25<br>81+36+36<br>121+16+16 | $2y^2+2yz+77z^2=\begin{cases}(y+3z)^2+(y-2z)^2+64z^2\\(y+5z)^2+(y-4z)^2+36z^2\\(y+6z)^2+(y-5z)^2+16z^2\end{cases}$ |
| 100+49+4<br>100+49+4<br>144+9 | $9y^2+18yz+26z^2=\begin{cases}(2y+5z)^2+4y^2+(y-z)^2\\(2y+4z)^2+(2y-z)^2+(y+3z)^2\\(3y+3z)^2+16z^2+z^2\end{cases}$ |
| 144+9<br>81+36+36<br>81+36+36 | $y^2+2yz+154z^2=(y+z)^2+144z^2+9z^2$<br>$9y^2+6yz+18z^2=4y^2+(2y+3z)^2+(y-3z)^2$<br>$13y^2+18yz+18z^2=4y^2+9(y+z)^2+9z^2$ |

# TABLE VIII.

| NOMBRE $c$. | DIVISEURS $4n+1$. |
|---|---|
| | $t^2+157u^2$ |
| $121+36$<br>$144+9+4$ | $y^2+2yz+158z^2=(y+z)^2+121z^2+36z^2$<br>$13y^2+10yz+14z^2=(3y+3z)^2+(2y-2z)^2+z^2$ |
| | $t^2+161u^2$ |
| $100+36+25$<br>$81+64+16$ | $5y^2+6yz+34z^2=\begin{cases}4y^2+(y+3z)^2+25z^2\\(2y+3z)^2+(y-3z)^2+16z^2\end{cases}$ |
| $144+16+1$<br>$121+36+4$ | $10y^2+6yz+17z^2=\begin{cases}y^2+(3y+z)^2+16z^2\\(3y+2z)^2+(y-3z)^2+4z^2\end{cases}$ |
| | $y^2+2yz+162z^2$, $2y^2+2yz+81z^2$ *non décomposables.* |
| | $t^2+165u^2$ |
| $100+49+16$<br>$100+49+16$<br>$100+64+1$<br>$100+64+1$ | $29y^2+6yz+6z^2=\begin{cases}(5y+z)^2+(2y-z)^2+4z^2\\(3y+z)^2+(4y-z)^2+(2y+2z)^2\\(4y+2z)^2+(3y-z)^2+(2y-z)^2\\(4y+z)^2+(3y+z)^2+(2y-2z)^2\end{cases}$ |
| | $y^2+2yz+166z^2$, $5y^2+10yz+38z^2$, $13y^2+22yz+22z^2$ *non décomposables.* |
| | $t^2+169u^2$ |
| $144+25$<br>$169$ | $y^2+2yz+170z^2=\begin{cases}(y+z)^2+144z^2+25z^2\\(y+z)^2+169z^2\end{cases}$ |
| $144+16+9$<br>$169$ | $17y^2+2yz+10z^2=\begin{cases}(y+z)^2+16y^2+9z^2\\(4y+z)^2+(y-3z)^2\end{cases}$ |
| $169$<br>$169$ | $2y^2+2yz+85z^2=(y+7z)^2+(y-6z)^2$<br>$34y^2+2yz+5z^2=(5y-z)^2+(3y+2z)^2$ |
| | $t^2+173u^2$ |
| $169+4$<br>$144+25+4$<br>$121+36+16$<br>$100+64+9$ | $y^2+2yz+174z^2=(y+z)^2+169z^2+4z^2$<br>$6y^2+2yz+29z^2=y^2+(y+5z)^2+(2y-2z)^2$<br>$13y^2+6yz+14z^2=(3y-z)^2+(2y+3z)^2+4z^2$<br>$9y^2+10yz+22z^2=(2y+3z)^2+(y+3z)^2+(2y-2z)^2$ |

## TABLE VIII.

| NOMBRE $c$. | DIVISEURS $4n+1$. |
|---|---|
| | $t^2+177u^2$ |
| 64+64+49<br>169+4+4 | $2y^2+2yz+89z^2=\begin{cases}(y+4z)^2+(y-3z)^2+64z^2\\(y+7z)^2+(y-6z)^2+4z^2\end{cases}$ |
| | $y^2+2yz+178z^2$ *non décomposable.* |
| | $t^2+181u^2$ |
| 100+81 | $y^2+2yz+182z^2=(y+z)^2+100z^2+81z^2$ |
| 144+36+1 | $5y^2+6yz+38z^2=(2y+z)^2+(y+z)^2+36z^2$ |
| 81+64+36 | $13y^2+2yz+14z^2=(3y-z)^2+(2y+2z)^2+9z^2$ |
| | $t^2+185u^2$ |
| 169+16<br>121+64 | $y^2+2yz+186z^2=\begin{cases}(y+z)^2+169z^2+16z^2\\(y+z)^2+121z^2+64z^2\end{cases}$ |
| 144+25+16 | $10y^2+10yz+21z^2=\begin{cases}(3y+2z)^2+(y-z)^2+16z^2\\(3y+z)^2+(y+2z)^2+16z^2\end{cases}$ |
| 100+81+4<br>100+49+36 | $9y^2+14yz+26z^2=\begin{cases}(2y+z)^2+4y^2+(y+5z)^2\\(2y+4z)^2+(2y+z)^2+(y-3z)^2\end{cases}$ |
| | $\left.\begin{array}{l}2y^2+2yz+93z^2\\5y^2+10yz+42z^2\\18y^2+14yz+13z^2\end{array}\right\}$ *non décomposables.* |
| | $t^2+189u^2$ |
| 169+16+4<br>100+64+25<br>144+36+9<br>144+36+9 | $5y^2+2yz+38z^2=\begin{cases}(2y+3z)^2+(y-5z)^2+4z^2\\(2y+2z)^2+(y-3z)^2+25z^2\\(2y+z)^2+(y-z)^2+36z^2\\(2y-2z)^2+(y+5z)^2+9z^2\end{cases}$ |
| 121+64+4<br>144+36+9<br>121+64+4<br>144+36+9 | $17y^2+14yz+14z^2=\begin{cases}(4y+z)^2+(y+3z)^2+4z^2\\(4y+2z)^2+(y-z)^2+9z^2\\(3y-z)^2+(2y+3z)^2+(2y+2z)^2\\(3y+3z)^2+(2y+z)^2+(2y-2z)^2\end{cases}$ |
| | $\left.\begin{array}{l}y^2+2yz+190z^2\\9y^2+6yz+22z^2\\9y^2+18yz+30z^2\end{array}\right\}$ *non décomposables.* |
| 144+36+9 | $33y^2+6yz+6z^2=(2y+z)^2+(5y+z)^2+(2y-2z)^2$ |
| | $t^2+103u^2$ |
| 144+49 | $y^2+2yz+194z^2=(y+z)^2+144z^2+49z^2$ |
| 121+36+36 | $2y^2+2yz+97z^2=(y+6z)^2+(y-5z)^2+36z^2$ |

## TABLE VIII.

| NOMBRE *c.* | DIVISEURS $4n+1$. |
| --- | --- |
| | $\underbrace{t^2 + 197u^2}$ |
| 196+1<br>144+49+4<br>100+81+16 | $y^2+2yz+198z^2=(y+z)^2+196z^2+z^2$<br>$6y^2+2yz+33z^2=(y-5z)^2+(y+2z)^2+(2y+2z)^2$<br>$9y^2+2yz+22z^2=(2y+2z)^2+(2y-3z)^2+(y+3z)^2$ |
| | $\underbrace{t^2 + 201u^2}$ |
| 100+100+1<br>169+16+16 | $2y^2+2yz+101z^2=\begin{cases}y^2+(y+z)^2+100z^2\\(y+7z)^2+(y-6z)^2+16z^2\end{cases}$ |
| 196+4+1<br>121+64+16 | $5y^2+6yz+42z^2=\begin{cases}(2y+4z)^2+(y-5z)^2+z^2\\(2y-z)^2+(y+5z)^2+16z^2\end{cases}$ |
| | $\left.\begin{matrix}y^2+2yz+202z^2\\10y^2+6yz+21z^2\end{matrix}\right\}$ *non décomposables.* |
| | $\underbrace{t^2 + 205u^2}$ |
| 196+9<br>169+36 | $y^2+2yz+206z^2=\begin{cases}(y+z)^2+196z^2+9z^2\\(y+z)^2+169z^2+36z^2\end{cases}$ |
| 144+36+25 | $5y^2+10yz+46z^2=\begin{cases}(2y+z)^2+(y+3z)^2+36z^2\\(2y+3z)^2+(y-z)^2+36z^2\end{cases}$ |
| | $13y^2+18yz+22z^2$ *non décomposable.* |
| | $\underbrace{t^2 + 209u^2}$ |
| 100+100+9<br>64+64+81 | $2y^2+2yz+105z^2=\begin{cases}(y+2z)^2+(y-z)^2+100z^2\\(y+5z)^2+(y-4z)^2+64z^2\end{cases}$ |
| 169+36+4<br>144+49+16 | $10y^2+2yz+21z^2=\begin{cases}(3y-z)^2+(y+4z)^2+4z^2\\(3y+z)^2+(y-2z)^2+16z^2\end{cases}$ |
| 144+64+1<br>196+9+4 | $13y^2+10yz+18z^2=\begin{cases}(3y+z)^2+(2y+z)^2+16z^2\\(3y-z)^2+(2y+4z)^2+z^2\end{cases}$ |
| | $\left.\begin{matrix}y^2+2yz+210z^2\\5y^2+2yz+42z^2\\9y^2+10yz+26z^2\end{matrix}\right\}$ *non décomposables.* |
| | $\underbrace{t^2 + 213u^2}$ |
| 196+16+1<br>100+64+49 | $17y^2+10yz+14z^2=\begin{cases}(4y+2z)^2+(y-3z)^2+z^2\\(2y+3z)^2+(2y-2z)^2+(3y+z)^2\end{cases}$ |
| | $\left.\begin{matrix}y^2+2yz+214z^2\\37y^2+6yz+6z^2\end{matrix}\right\}$ *non décomposables.* |

# TABLE IX.

DIVISEURS $4n+2$ de la formule $t^2+cu^2$, $c$ étant un nombre de la forme $8n+3$.

| NOMBRE C. | DIVISEURS $4n+2$. |
| --- | --- |
| $1+1+1$ | $t^2+3u^2$<br>$2y^2+2yz+2z^2=(y+z)^2+y^2+z^2$ |
| $9+1+1$ | $t^2+11u^2$<br>$2y^2+2yz+6z^2=(y+2z)^2+(y-z)^2+z^2$ |
| $9+9+1$ | $t^2+19u^2$<br>$2y^2+2yz+10z^2=y^2+(y+z)^2+9z^2$ |
| $25+1+1$<br>$9+9+9$ | $t^2+27u^2$<br>$2y^2+2yz+14z^2=\begin{cases}(y+3z)^2+(y-2z)^2+z^2\\(y+2z)^2+(y-z)^2+9z^2\end{cases}$ |
| $9+9+9$ | $6y^2+6yz+6z^2=(2y+z)^2+(y+2z)^2+(y-z)^2$ |
| $25+9+1$ | $t^2+35u^2$<br>$6y^2+2yz+6z^2=\begin{cases}(2y+z)^2+(y+z)^2+(y-2z)^2\\(y+2z)^2+(y+z)^2+(2y-z)^2\end{cases}$<br>$2y^2+2yz+18z^2$ *non décomposable.* |
| $25+9+9$ | $t^2+43u^2$<br>$2y^2+2yz+22z^2=(y+3z)^2+(y-2z)^2+9z^2$ |
| $25+25+1$<br>$49+1+1$ | $t^2+51u^2$<br>$2y^2+2yz+26z^2=\begin{cases}y^2+(y+z)^2+25z^2\\(y+4z)^2+(y-3z)^2+z^2\end{cases}$<br>$6y^2+6yz+10z^2$ *non décomposable.* |
| $25+25+9$<br>$49+9+1$ | $t^2+59u^2$<br>$2y^2+2yz+30z^2=(y+2z)^2+(y-z)^2+25z^2$<br>$6y^2+2yz+10z^2=(y+3z)^2+(2y-z)^2+y^2$ |
| $49+9+9$ | $t^2+67u^2$<br>$2y^2+2yz+34z^2=(y+4z)^2+(y-3z)^2+9z^2$ |

# TABLE IX.

| NOMBRE $c$. | DIVISEURS $4n+2$. |
|---|---|
| | $t^2 + 75u^2$ |
| 49+25+1<br>49+25+1<br>25+25+25 | $6y^2+6yz+14z^2 = \begin{cases}(2y+3z)^2+(y-2z)^2+(y-z)^2\\(2y-z)^2+(y+3z)^2+(y+2z)^2\\(2y+z)^2+(y+3z)^2+(y-2z)^2\end{cases}$ |
| | $10y^2+10yz+10z^2$ *non décomposable.* |
| 25+25+25 | $2y^2+2yz+38z^2 = (y+3z)^2+(y-2z)^2+25z^2$ |
| | $t^2 + 83u^2$ |
| 81+1+1 | $2y^2+2yz+42z^2 = (y+5z)^2+(y-4z)^2+z^2$ |
| 49+25+9 | $6y^2+2yz+14z^2 = (2y+z)^2+(y+2z)^2+(y-3z)^2$ |
| | $t^2 + 91u^2$ |
| 81+9+1 | $10y^2+6yz+10z^2 = \begin{cases}y^2+(3y+z)^2+9z^2\\z^2+(3z+y)^2+9y^2\end{cases}$ |
| | $2y^2+2yz+46z^2$ *non décomposable.* |
| | $t^2 + 99u^2$ |
| 49+49+1<br>49+25+25<br>81+9+9 | $2y^2+2yz+50z^2 = \begin{cases}y^2+(y+z)^2+49z^2\\(y+4z)^2+(y-3z)^2+25z^2\\(y+5z)^2+(y-4z)^2+9z^2\end{cases}$ |
| 81+9+9 | $10y^2+2yz+10z^2 = (y+z)^2+9y^2+9z^2$ |
| 81+9+9 | $6y^2+6yz+18z^2 = y^2+(2y+3z)^2+(y-3z)^2$ |
| | $t^2 + 107u^2$ |
| 49+49+9 | $2y^2+2yz+54z^2 = (y+2z)^2+(y-z)^2+49z^2$ |
| 81+25+1 | $6y^2+2yz+18z^2 = (2y-z)^2+(y-z)^2+(y+4z)^2$ |
| | $t^2 + 115u^2$ |
| 81+25+9 | $10y^2+10yz+14z^2 = \begin{cases}(3y+z)^2+(y+2z)^2+9z^2\\(3y+2z)^2+(y-z)^2+9z^2\end{cases}$ |
| | $2y^2+2yz+58z^2$ *non décomposable.* |
| | $t^2 + 123u^2$ |
| 49+49+25<br>121+1+1 | $2y^2+2yz+62z^2 = \begin{cases}(y+3z)^2+(y-2z)^2+49z^2\\(y+6z)^2+(y-5z)^2+z^2\end{cases}$ |
| | $6y^2+6yz+22z^2$ *non décomposable.* |

## TABLE IX.

| NOMBRE $c$. | DIVISEURS $4n+2$. |
|---|---|
| | $t^2 + 131\,u^2$ |
| $81+25+25$ | $2y^2+2yz+66z^2=(y+5z)^2+(y-4z)^2+25z^2$ |
| $81+49+1$ | $6y^2+2yz+22z^2=(2y+3z)^2+(y-3z)^2+(y-2z)^2$ |
| $121+9+1$ | $10y^2+6yz+14z^2=(3y+2z)^2+(y-3z)^2+z^2$ |
| | $t^2 + 139\,u^2$ |
| $121+9+9$ | $2y^2+2yz+70z^2=(y+6z)^2+(y-5z)^2+9z^2$ |
| $81+49+9$ | $10y^2+2yz+14z^2=(3y+z)^2+(y-2z)^2+9z^2$ |
| | $t^2 + 147\,u^2$ |
| $121+25+1$<br>$121+25+1$<br>$49+49+49$ | $6y^2+6yz+26z^2=\begin{cases}(y+z)^2+(y-4z)^2+(2y+3z)^2\\(2y-z)^2+(y+5z)^2+y^2\\(2y+z)^2+(y+4z)^2+(y-3z)^2\end{cases}$ |
| $49+49+49$ | $2y^2+2yz+74z^2=(y+4z)^2+(y-3z)^2+49z^2$ |
| $49+49+49$ | $14y^2+14yz+14z^2=(3y+z)^2+(2y+3z)^2+(y-2z)^2$ |
| | $t^2 + 155\,u^2$ |
| $121+25+9$<br>$81+49+25$ | $6y^2+2yz+26z^2=\begin{cases}(2y+3z)^2+(y-4z)^2+(y-z)^2\\(2y+z)^2+(y+3z)^2+(y-4z)^2\end{cases}$ |
| | $\left.\begin{matrix}2y^2+2yz+78z^2\\10y^2+10yz+18z^2\end{matrix}\right\}$ *non décomposables.* |
| | $t^2 + 163\,u^2$ |
| $81+81+1$ | $2y^2+2yz+82z^2=y^2+(y+z)^2+81z^2$ |
| | $t^2 + 171\,u^2$ |
| $121+25+25$<br>$169+1+1$<br>$81+81+9$ | $2y^2+2yz+86z^2=\begin{cases}(y+6z)^2+(y-5z)^2+25z^2\\(y+7z)^2+(y-6z)^2+z^2\\(y+2z)^2+(y-z)^2+81z^2\end{cases}$ |
| $121+49+1$<br>$121+49+1$<br>$81+81+9$ | $14y^2+10yz+14z^2=\begin{cases}(3y+2z)^2+(2y+z)^2+(y-3z)^2\\(3y-z)^2+(y+2z)^2+(2y+3z)^2\\(3y+3z)^2+(2y-z)^2+(y-2z)^2\end{cases}$ |
| | $6y^2+6yz+30z^2$ *non décomposable.* |
| $81+81+9$ | $10y^2+6yz+18z^2=9y^2+(y+3z)^2+9z^2$ |

## TABLE IX.

| NOMBRE C. | DIVISEURS $4n+2$. |
|---|---|
| | $t^2 + 179u^2$ |
| 81+49+49<br>121+49+9<br>169+9+1 | $2y^2+2yz+90z^2=(y+5z)^2+(y-4z)^2+49z^2$<br>$6y^2+2yz+30z^2=(2y-z)^2+(y-2z)^2+(y+5z)^2$<br>$10y^2+2yz+18z^2=(3y-z)^2+(y+4z)^2+z^2$ |
| | $t^2 + 187u^2$ |
| 81+81+25<br>169+9+9 | $2y^2+2yz+94z^2=\begin{cases}(y+3z)^2+(y-2z)^2+81z^2\\(y+7z)^2+(y-6z)^2+9z^2\end{cases}$<br>$14y^2+6yz+14z^2$ *non décomposable.* |
| | $t^2 + 195u^2$ |
| 169+25+1<br>121+49+25<br>169+25+1<br>121+49+25 | $14y^2+2yz+14z^2=\begin{cases}(3y+2z)^2+(2y-3z)^2+(y+z)^2\\(3y+2z)^2+(2y-z)^2+(y-3z)^2\\(3y-2z)^2+(2y+3z)^2+(y+z)^2\\(3y-z)^2+(2y+3z)^2+(y-2z)^2\end{cases}$<br>$\left.\begin{array}{l}2y^2+2yz+98z^2\\6y^2+6yz+34z^2\\10y^2+10yz+22z^2\end{array}\right\}$ *non décomposables.* |
| | $t^2 + 203u^2$ |
| 169+25+9<br>121+81+1 | $6y^2+2yz+34z^2=\begin{cases}(2y+3z)^2+(y-5z)^2+y^2\\(2y-3z)^2+(y+4z)^2+(y+3z)^2\end{cases}$<br>$\left.\begin{array}{l}2y^2+2yz+102z^2\\14y^2+14yz+18z^2\end{array}\right\}$ *non décomposables.* |
| | $t^2 + 211u^2$ |
| 81+81+49<br>121+81+9 | $2y^2+2yz+106z^2=(y+4z)^2+(y-3z)^2+81z^2$<br>$10y^2+6yz+22z^2=(3y+2z)^2+(y-3z)^2+9z^2$ |
| | $t^2 + 219u^2$ |
| 169+25+25<br>121+49+49<br>169+49+1 | $2y^2+2yz+110z^2=\begin{cases}(y+7z)^2+(y-6z)^2+25z^2\\(y+6z)^2+(y-5z)^2+49z^2\end{cases}$<br>$6y^2+6yz+38z^2=\begin{cases}(2y-z)^2+(y+6z)^2+(y-z)^2\\(2y+3z)^2+(y+2z)^2+(y-5z)^2\end{cases}$<br>$10y^2+2yz+22z^2$ *non décomposable.* |

# TABLE X.

Diviseurs $8n+1, 8n+3$ de la formule $t^2+2au^2$, $a$ étant de la forme $4n+1$.

| NOMBRE $2a$. | DIVISEURS $8n+1$, $8n+3$. |
| --- | --- |
| | $\overbrace{t^2 + 2u^2}$ |
| 1+1 | $y^2+2z^2=y^2+z^2+z^2$ |
| | $\overbrace{t^2 + 10u^2}$ |
| 9+1 | $y^2+10z^2=y^2+9z^2+z^2$ |
| | $\overbrace{t^2 + 18u^2}$ |
| 16+1+1<br>9+9 | $2y^2+9z^2=\begin{cases}(y+2z)^2+(y-2z)^2+z^2\\ y^2+y^2+9z^2\end{cases}$ |
| 9+9<br>9+9 | $y^2+18z^2=y^2+9z^2+9z^2$<br>$3y^2+6z^2=(y+2z)^2+(y-z)^2+(y-z)^2$ |
| | $\overbrace{t^2 + 26u^2}$ |
| 25+1<br>16+9+1 | $y^2+26z^2=y^2+25z^2+z^2$<br>$3y^2+4yz+10z^2=y^2+(y+3z)^2+(y-z)^2$ |
| | $\overbrace{t^2 + 34u^2}$ |
| 25+9<br>16+9+9 | $y^2+34z^2=y^2+25z^2+9z^2$<br>$2y^2+17z^2=(y+2z)^2+(y-2z)^2+9z^2$ |
| | $\overbrace{t^2 + 42u^2}$ |
| 25+16+1 | $3y^2+14z^2=\begin{cases}(y-2z)^2+(y+3z)^2+(y-z)^2\\ (y+2z)^2+(y-3z)^2+(y+z)^2\end{cases}$<br>$y^2+42z^2$ *non décomposable.* |
| | $\overbrace{t^2 + 50u^2}$ |
| 49+1<br>25+25 | $y^2+50z^2=\begin{cases}y^2+49z^2+z^2\\ y^2+25z^2+25z^2\end{cases}$ |
| 25+25 | $2y^2+25z^2=y^2+y^2+25z^2$ |
| | $\overbrace{t^2 + 58u^2}$ |
| 49+9 | $y^2+58z^2=y^2+49z^2+9z^2$ |

| NOMBRE 2*a*. | DIVISEURS $8n+1, 8n+3$. |
|---|---|
| | $t^2 + 66\,u^2$ |
| $64+1+1$<br>$25+25+16$ | $2y^2+33z^2 = \begin{cases}(y+4z)^2+(y-4z)^2+z^2\\(y+2z)^2+(y-2z)^2+25z^2\end{cases}$ |
| $49+16+1$ | $6y^2+11z^2 = \begin{cases}(2y+z)^2+(y-3z)^2+(y+z)^2\\(2y-z)^2+(y+3z)^2+(y-z)^2\end{cases}$ |
| | $\left.\begin{matrix}y^2+66z^2\\3y^2+22z^2\end{matrix}\right\}$ *non décomposables.* |
| | $t^2 + 74\,u^2$ |
| $25+49$<br>$49+16+9$<br>$64+9+1$ | $y^2+74z^2 = y^2+25z^2+49z^2$<br>$3y^2+4yz+26z^2 = (y+4z)^2+(y+z)^2+(y-3z)^2$<br>$9y^2+8yz+10z^2 = (2y+3z)^2+(2y-z)^2+y^2$ |
| | $t^2 + 82\,u^2$ |
| $81+1$<br>$64+9+9$ | $y^2+82z^2 = y^2+z^2+81z^2$<br>$2y^2+41z^2 = (y+4z)^2+(y-4z)^2+9z^2$ |
| | $t^2 + 90\,u^2$ |
| $64+25+1$<br>$49+25+16$<br>$81+9$ | $9y^2+12yz+14z^2 = \begin{cases}(2y+3z)^2+(2y-z)^2+(y+2z)^2\\(2y+3z)^2+(2y+z)^2+(y-2z)^2\\(3y+2z)^2+9z^2+z^2\end{cases}$ |
| | $3y^2+30z^2$ *non décomposable.* |
| $81+9$<br>$81+9$ | $y^2+90z^2 = y^2+81z^2+9z^2$<br>$10y^2+9z^2 = y^2+9y^2+9z^2$ |
| | $t^2 + 98\,u^2$ |
| $64+25+9$<br>$49+49$ | $3y^2+4yz+34z^2 = \begin{cases}(y-3z)^2+(y+5z)^2+y^2\\(y+3z)^2+(y+3z)^2+(y-4z)^2\end{cases}$ |
| $81+16+1$<br>$49+49$ | $6y^2+4yz+17z^2 = \begin{cases}y^2+(2y-z)^2+(y+4z)^2\\(2y+3z)^2+(y-2z)^2+(y-2z)^2\end{cases}$ |
| $49+49$<br>$49+49$<br>$49+49$ | $y^2+98z^2 = y^2+49z^2+49z^2$<br>$2y^2+49z^2 = y^2+y^2+49z^2$<br>$9y^2+16yz+18z^2 = (2y+z)^2+(2y+z)^2+(y+4z)^2$ |

## TABLE X.

| NOMBRE 2a. | DIVISEURS $8n+1, 8n+3$. |
| --- | --- |
| | $\underbrace{t^2 + 106u^2}$ |
| 81+25<br>81+16+9 | $y^2+106z^2=y^2+81z^2+25z^2$<br>$10y^2+4yz+11z^2=(y-z)^2+(3y+z)^2+9z^2$ |
| | $\underbrace{t^2 + 114u^2}$ |
| 49+49+16<br>25+25+64 | $2y^2+57z^2=\begin{cases}(y+2z)^2+(y-2z)^2+49z^2\\(y+4z)^2+(y-4z)^2+25z^2\end{cases}$ |
| 64+49+1 | $3y^2+38z^2=\begin{cases}(y+5z)^2+(y-3z)^2+(y-2z)^2\\(y-5z)^2+(y+3z)^2+(y+2z)^2\end{cases}$ |
| | $\left.\begin{array}{l}y^2+114z^2\\6y^2+19z^2\end{array}\right\}$ *non décomposables.* |
| | $\underbrace{t^2 + 122u^2}$ |
| 121+1<br>81+25+16<br>64+49+9 | $y^2+122z^2=y^2+121z^2+z^2$<br>$3y^2+4yz+42z^2=(y+5z)^2+(y-4z)^2+(y+z)^2$<br>$9y^2+4yz+14z^2=(2y+3z)^2+(2y-z)^2+(y-2z)^2$ |
| | $\underbrace{t^2 + 130u^2}$ |
| 121+9<br>81+49 | $y^2+130z^2=\begin{cases}y^2+121z^2+9z^2\\y^2+81z^2+49z^2\end{cases}$ |
| | $2y^2+65z^2$ *non décomposable.* |
| | $\underbrace{t^2 + 138u^2}$ |
| 64+49+25<br>121+16+1 | $11y^2+8yz+14z^2=\begin{cases}(3y+z)^2+(y-2z)^2+(y+3z)^2\\(3y+2z)^2+(y-3z)^2+(y+z)^2\end{cases}$ |
| | $\left.\begin{array}{l}y^2+138z^2\\3y^2+46z^2\end{array}\right\}$ *non décomposables.* |
| | $\underbrace{t^2 + 146u^2}$ |
| 121+25<br>144+1+1<br>81+64+1<br>121+16+9<br>81+49+16 | $y^2+146z^2=y^2+121z^2+25z^2$<br>$2y^2+73z^2=(y+6z)^2+(y-6z)^2+z^2$<br>$3y^2+4yz+50z^2=(y+4z)^2+(y+3z)^2+(y-5z)^2$<br>$6y^2+4yz+25z^2=y^2+(2y+3z)^2+(y-4z)^2$<br>$9y^2+8yz+18z^2=(2y+z)^2+(2y-z)^2+(y+4z)^2$ |

TABLE X.

| NOMBRE 2a. | DIVISEURS $8n+1, 8n+3$. |
|---|---|
| | $t^2 + 154u^2$ |
| 144+9+1<br>81+64+9 | $17y^2+8yz+10z^2 = \begin{cases} y^2+(4y+z)^2+9z^2 \\ 9y^2+(2y-z)^2+(2y+3z)^2 \end{cases}$ |
| | $\left.\begin{matrix} y^2+154z^2 \\ 11y^2+14z^2 \end{matrix}\right\}$ *non décomposables.* |
| | $t^2 + 162u^2$ |
| 144+9+9<br>121+25+16<br>81+81 | $11y^2+12yz+18z^2 = \begin{cases} (3y+3z)^2+(y-3z)^2+y^2 \\ (y-z)^2+(3y+z)^2+(y+4z)^2 \\ 9y^2+(y+3z)^2+(y+3z)^2 \end{cases}$ |
| 81+81<br>64+49+49<br>144+9+9 | $2y^2+81z^2 = \begin{cases} y^2+y^2+81z^2 \\ (y+4z)^2+(y-4z)^2+49z^2 \\ (y+6z)^2+(y-6z)^2+9z^2 \end{cases}$ |
| 81+81 | $y^2+162z^2 = y^2+81z^2+81z^2$ |
| 144+9+9 | $9y^2+18z^2 = (2y+3z)^2+(2y-3z)^2+y^2$ |
| 81+81 | $9y^2+12yz+22z^2 = (3y+2z)^2+9z^2+9z^2$ |
| 81+81 | $3y^2+54z^2 = (y+3z)^2+(y+3z)^2+(y-6z)^2$ |
| 81+81 | $6y^2+27z^2 = (2y+3z)^2+(y-3z)^2+(y-3z)^2$ |
| | $t^2 + 170u^2$ |
| 169+1<br>121+49 | $y^2+170z^2 = \begin{cases} y^2+169z^2+z^2 \\ y^2+121z^2+49z^2 \end{cases}$ |
| 144+25+1<br>81+64+25 | $9y^2+16yz+26z^2 = \begin{cases} (2y+5z)^2+(2y-z)^2+y^2 \\ (2y+3z)^2+(2y-z)^2+(y+4z)^2 \end{cases}$ |
| | $\left.\begin{matrix} 10y^2+17z^2 \\ 3y^2+4yz+58z^2 \end{matrix}\right\}$ *non décomposables.* |
| | $t^2 + 178u^2$ |
| 169+9 | $y^2+178z^2 = y^2+169z^2+9z^2$ |
| 81+81+16 | $2y^2+89z^2 = (y+2z)^2+(y-2z)^2+81z^2$ |
| 144+25+9 | $11y^2+16yz+22z^2 = (3y+3z)^2+(y-3z)^2+(y+2z)^2$ |
| | $t^2 + 186u^2$ |
| 169+16+1<br>121+64+1 | $11y^2+20yz+26z^2 = \begin{cases} (y+z)^2+(y-3z)^2+(3y+4z)^2 \\ (3y+z)^2+(y+4z)^2+(y+3z)^2 \end{cases}$ |
| 121+49+16 | $3y^2+62z^2 = \begin{cases} (y-z)^2+(y+6z)^2+(y-5z)^2 \\ (y+z)^2+(y-6z)^2+(y+5z)^2 \end{cases}$ |
| | $\left.\begin{matrix} y^2+186z^2 \\ 10y^2+4yz+19z^2 \end{matrix}\right\}$ *non décomposables.* |

# TABLE X.

| NOMBRE $2a$. | DIVISEURS $8n+1, 8n+3$. |
| --- | --- |
| | $t^2 + 194u^2$ |
| $169+25$ | $y^2+194z^2 = y^2+169z^2+25z^2$ |
| $144+25+25$ | $2y^2+97z^2 = (y+6z)^2+(y-6z)^2+25z^2$ |
| $121+64+9$ | $3y^2+4yz+66z^2 = (y+7z)^2+(y-4z)^2+(y-z)^2$ |
| $81+64+49$ | $6y^2+4yz+33z^2 = (2y+z)^2+(y+4z)^2+(y-4z)^2$ |
| $144+49+1$ | $9y^2+4yz+22z^2 = (2y+3z)^2+(2y-3z)^2+(y+2z)^2$ |
| $169+16+9$ | $18y^2+4yz+11z^2 = (4y+z)^2+(y-3z)^2+(y+z)^2$ |
| | $t^2 + 202u^2$ |
| $121+81$ | $y^2+202z^2 = y^2+121z^2+81z^2$ |
| $144+49+9$ | $17y^2+12yz+14z^2 = (4y+z)^2+(y+2z)^2+9z^2$ |
| | $t^2 + 210u^2$ |
| $169+25+16$ <br> $121+64+25$ | $35y^2+6z^2 = \begin{cases}(5y\pm z)^2+(3y\mp 2z)^2+(y\pm z)^2 \\ (5y\pm z)^2+(3y\mp z)^2+(y\mp 2z)^2\end{cases}$ |
| | $y^2+210z^2$, $2y^2+105z^2$, $70y^2+3z^2$ } *non décomposables.* |
| | $t^2 + 218u^2$ |
| $169+49$ | $y^2+218z^2 = y^2+169z^2+49z^2$ |
| $121+81+16$ | $9y^2+8yz+26z^2 = (2y+3z)^2+(2y+z)^2+(y-4z)^2$ |
| | $t^2 + 226u^2$ |
| $225+1$ | $y^2+226z^2 = y^2+225z^2+z^2$ |
| $81+81+64$ | $2y^2+113z^2 = (y+4z)^2+(y-4z)^2+81z^2$ |
| $144+81+1$ | $11y^2+8yz+22z^2 = (3y+3z)^2+(y-3z)^2+(y-2z)^2$ |
| | $t^2 + 234u^2$ |
| $169+49+16$ <br> $169+64+1$ <br> $144+81+9$ | $17y^2+4yz+14z^2 = \begin{cases}(3y-2z)^2+(2y+z)^2+(2y+3z)^2 \\ (3y+2z)^2+(2y+z)^2+(2y-3z)^2 \\ (4y+z)^2+(y-2z)^2+9z^2\end{cases}$ |
| $121+64+49$ <br> $121+64+49$ <br> $225+9$ | $9y^2+26z^2 = \begin{cases}(y-4z)^2+(2y-z)^2+(2y+3z)^2 \\ (y+4z)^2+(2y+z)^2+(2y-3z)^2 \\ 9y^2+25z^2+z^2\end{cases}$ |
| $225+9$ | $y^2+234z^2 = y^2+225z^2+9z^2$ |
| $144+81+9$ | $3y^2+78z^2 = (y+7z)^2+(y-5z)^2+(y-2z)^2$ |
| | &c. &c. &c. |

# TABLE XI.

Diviseurs $8n+3$, $8n+5$ de la formule $t^2+2au^2$, $a$ étant de la forme $4n-1$.

| NOMBRE $2a$. | DIVISEURS $8n+3, 8n+5$. |
|---|---|
| | $t^2+6u^2$ |
| $4+1+1$ | $2y^2+3z^2=(y+z)^2+(y-z)^2+z^2$ |
| | $t^2+14u^2$ |
| $9+4+1$ | $3y^2+4yz+6z^2=(y+z)^2+(y+2z)^2+(y-z)^2$ |
| | $t^2+22u^2$ |
| $9+9+4$ | $2y^2+11z^2=(y+z)^2+(y-z)^2+9z^2$ |
| | $t^2+30u^2$ |
| $25+4+1$ | $5y^2+6z^2=\begin{cases}(y+2z)^2+(2y-z)^2+z^2\\(y-2z)^2+(2y+z)^2+z^2\end{cases}$ |
| | $10y^2+3z^2$ *non décomposable.* |
| | $t^2+38u^2$ |
| $36+1+1$ | $2y^2+19z^2=(y+3z)^2+(y-3z)^2+z^2$ |
| $25+9+4$ | $3y^2+4yz+14z^2=(y+3z)^2+(y+z)^2+(y-2z)^2$ |
| | $t^2+46u^2$ |
| $36+9+1$ | $5y^2+4yz+10z^2=(2y+z)^2+y^2+9z^2$ |
| | $t^2+54u^2$ |
| $36+9+9$<br>$25+25+4$ | $2y^2+27z^2=\begin{cases}(y+3z)^2+(y-3z)^2+9z^2\\(y+z)^2+(y-z)^2+25z^2\end{cases}$ |
| $49+4+1$<br>$36+9+9$ | $5y^2+8yz+14z^2=\begin{cases}(2y+3z)^2+(y-2z)^2+z^2\\(2y+z)^2+(y+2z)^2+9z^2\end{cases}$ |
| $36+9+9$ | $3y^2+18z^2=(y+3z)^2+(y-3z)^2+y^2$ |
| | $t^2+62u^2$ |
| $49+9+4$ | $6y^2+4yz+11z^2=(y+z)^2+(y+3z)^2+(2y-z)^2$ |
| $36+25+1$ | $3y^2+4yz+22z^2=(y+3z)^2+(y-3z)^2+(y+2z)^2$ |

# TABLE XI.

| NOMBRE $2a$. | DIVISEURS $8n+3, 8n+5$. |
|---|---|
| 36+25+9 | $t^2+70u^2$<br>$5y^2+14z^2=\begin{cases}(2y+z)^2+(y-2z)^2+9z^2\\(2y-z)^2+(y+2z)^2+9z^2\end{cases}$<br>$2y^2+35z^2$ *non décomposable.* |
| 49+25+4 | $t^2+78u^2$<br>$3y^2+26z^2=\begin{cases}(y+4z)^2+(y-3z)^2+(y-z)^2\\(y-4z)^2+(y+3z)^2+(y+z)^2\end{cases}$<br>$6y^2+13z^2$ *non décomposable.* |
| 36+25+25<br>81+4+1<br>49+36+1 | $t^2+86u^2$<br>$2y^2+43z^2=(y+3z)^2+(y-3z)^2+25z^2$<br>$5y^2+4yz+18z^2=(2y-z)^2+(y+4z)^2+z^2$<br>$3y^2+4yz+30z^2=(y+5z)^2+(y-2z)^2+(y-z)^2$ |
| 49+36+9<br>81+9+4 | $t^2+94u^2$<br>$5y^2+8yz+22z^2=(2y+3z)^2+(y-2z)^2+9z^2$<br>$10y^2+8yz+11z^2=(3y+z)^2+(y+z)^2+9z^2$ |
| 100+1+1<br>49+49+4 | $t^2+102u^2$<br>$2y^2+51z^2=\begin{cases}(y+5z)^2+(y-5z)^2+z^2\\(y+z)^2+(y-z)^2+49z^2\end{cases}$<br>$3y^2+34z^2$ *non décomposable.* |
| 100+9+1<br>81+25+4<br>49+36+25 | $t^2+110u^2$<br>$10y^2+11z^2=\begin{cases}(3y+z)^2+(y-3z)^2+z^2\\(3y-z)^2+(y+3z)^2+z^2\end{cases}$<br>$6y^2+4yz+19z^2=\begin{cases}(2y+3z)^2+(y-3z)^2+(y-z)^2\\(2y+z)^2+(y+3z)^2+(y-3z)^2\end{cases}$<br>$\left.\begin{matrix}5y^2+22z^2\\3y^2+4yz+38z^2\end{matrix}\right\}$ *non décomposables.* |
| 100+9+9<br>81+36+1 | $t^2+118u^2$<br>$2y^2+59z^2=(y+5z)^2+(y-5z)^2+9z^2$<br>$11y^2+12yz+14z^2=(y-z)^2+(y-2z)^2+(3y+3z)^2$ |

## TABLE XI.

| NOMBRE 2*a*. | DIVISEURS $8n+3, 8n+5$. |
|---|---|
| | $t^2 + 126u^2$ |
| 121+4+1 | $5y^2+4yz+26z^2 = (y-4z)^2+(2y+3z)^2+z^2$ |
| 100+25+1 | $= y^2+(2y+z)^2+25z^2$ |
| 81+36+9 | $= (2y-z)^2+(y+4z)^2+9z^2$ |
| | $3y^2+42z^2$, $6y^2+21z^2$ *non décomposables.* |
| 81+36+9 | $10y^2+4yz+13z^2 = 9y^2+(y+2z)^2+9z^2$ |
| | $t^2 + 134u^2$ |
| 49+49+36 | $2y^2+67z^2 = (y+3z)^2+(y-3z)^2+49z^2$ |
| 121+9+4 | $11y^2+16yz+18z^2 = (3y+z)^2+(y+4z)^2+(y+z)^2$ |
| 100+25+9 | $5y^2+8yz+30z^2 = (y+2z)^2+(2y+z)^2+25z^2$ |
| 81+49+4 | $3y^2+4yz+46z^2 = (y-z)^2+(y+6z)^2+(y-3z)^2$ |
| | $t^2 + 142u^2$ |
| 81+36+25 | $11y^2+20yz+22z^2 = (3y+3z)^2+(y+3z)^2+(y-2z)^2$ |
| | $t^2 + 150u^2$ |
| 121+25+4 | $11y^2+4yz+14z^2 = (3y+2z)^2+(y-z)^2+(y-3z)^2$ |
| 100+49+1 | $= (3y-z)^2+(y+3z)^2+(y+2z)^2$ |
| 100+25+25 | $= (3y+z)^2+(y-3z)^2+(y+2z)^2$ |
| 100+25+25 | $2y^2+75z^2 = (y+5z)^2+(y-5z)^2+25z^2$ |
| 100+25+25 | $3y^2+50z^2 = (y+5z)^2+(y-5z)^2+y^2$ |
| 100+25+25 | $5y^2+30z^2 = (2y+z)^2+(y-2z)^2+25z^2$ |
| | $t^2 + 158u^2$ |
| 100+49+9 | $3y^2+4yz+54z^2 = (y+5z)^2+(y-5z)^2+(y+2z)^2$ |
| [illegible]1+36+1 | [illegible] $+4yz+27z^2 = (2y-z)^2+(y+5z)^2+(y-z)^2$ |
| | $t^2 + 166u^2$ |
| 81+8[illegible] | [illegible] $+83z^2 = (y+z)^2+(y-z)^2+81z^2$ |
| 121+[illegible] | [illegible] $y^2+4yz+34z^2 = (2y+3z)^2+(y-4z)^2+9z^2$ |
| 81+[illegible] | $13y^2+8yz+14z^2 = (3y+2z)^2+(2y-z)^2+9z^2$ |

# TABLE XI.

| NOMBRE $2a$. | DIVISEURS $8n+3$, $8n+5$. |
|---|---|
| | $t^2 + 174u^2$ |
| $121+49+4$ | $6y^2+29z^2 = \begin{cases}(y-4z)^2+(2y+3z)^2+(y-2z)^2\\(y+4z)^2+(2y-3z)^2+(y+2z)^2\end{cases}$ |
| $100+49+25$<br>$169+4+1$ | $5y^2+8yz+38z^2 = \begin{cases}(2y+3z)^2+(y-2z)^2+25z^2\\(2y-z)^2+(y+6z)^2+z^2\end{cases}$ |
| | $3y^2+58z^2$<br>$10y^2+8yz+19z^2$ } *non décomposables.* |
| | $t^2 + 182u^2$ |
| $169+9+4$ | $13y^2+14z^2 = \begin{cases}(3y+2z)^2+(2y-3z)^2+z^2\\(3y-2z)^2+(2y+3z)^2+z^2\end{cases}$ |
| $100+81+1$<br>$121+36+25$ | $3y^2+4yz+62z^2 = \begin{cases}(y+7z)^2+(y-3z)^2+(y-2z)^2\\(y+6z)^2+(y-5z)^2+(y+z)^2\end{cases}$ |
| | $2y^2+91z^2$ *non décomposable.* |
| | $t^2 + 190u^2$ |
| $100+81+9$ | $10y^2+19z^2 = \begin{cases}(3y+z)^2+(y-3z)^2+9z^2\\(3y-z)^2+(y+3z)^2+9z^2\end{cases}$ |
| | $5y^2+38z^2$ *non décomposable.* |
| | $t^2 + 198u^2$ |
| $196+1+1$<br>$100+49+49$<br>$81+81+36$ | $2y^2+99z^2 = \begin{cases}(y+7z)^2+(y-7z)^2+z^2\\(y+5z)^2+(y-5z)^2+49z^2\\(y+3z)^2+(y-3z)^2+81z^2\end{cases}$ |
| | $3y^2+66z^2$ *non décomposable.* |
| $81+81+36$ | $13y^2+12yz+18z^2 = 9y^2+9z^2+(2y+3z)^2$ |
| $81+81+36$ | $11y^2+18z^2 = (y+3z)^2+(y-3z)^2+9y^2$ |
| | $t^2 + 206u^2$ |
| $121+81+4$ | $3y^2+4yz+70z^2 = (y+5z)^2+(y+3z)^2+(y-6z)^2$ |
| $169+36+1$ | $6y^2+4yz+35z^2 = (2y+3z)^2+(y+z)^2+(y-5z)^2$ |
| $100+81+25$ | $5y^2+4yz+42z^2 = (2y-z)^2+(y+4z)^2+25z^2$ |
| $196+9+1$ | $10y^2+4yz+21z^2 = (3y+2z)^2+(y-4z)^2+z^2$ |
| $121+49+36$ | $11y^2+12yz+22z^2 = (3y+2z)^2+(y-3z)^2+(y+3z)^2$ |

TABLE XI.

| NOMBRE $2a$. | DIVISEURS $8n+3,\ 8n+5$. |
| --- | --- |
| | $t^2 + 214u^2$ |
| $196+9+9$ | $2y^2+107z^2=(y+7z)^2+(y-7z)^2+9z^2$ |
| $169+36+9$ | $5y^2+8yz+46z^2=(2y-z)^2+(y+6z)^2+9z^2$ |
| | $t^2 + 222u^2$ |
| $121+100+1$ | $3y^2+74z^2=\begin{cases}(y-7z)^2+(y+4z)^2+(y+3z)^2\\(y+7z)^2+(y-4z)^2+(y-3z)^2\end{cases}$ |
| $196+25+1$<br>$169+49+4$ | $11y^2+16yz+26z^2=\begin{cases}(3y+z)^2+(y+5z)^2+y^2\\(3y+4z)^2+(y-3z)^2+(y-z)^2\end{cases}$ |
| | $\left.\begin{matrix}6y^2+37z^2\\22y^2+16yz+13z^2\end{matrix}\right\}$ *non décomposables.* |
| | $t^2 + 230u^2$ |
| $225+4+1$ | $5y^2+46z^2=\begin{cases}(2y+3z)^2+(y-6z)^2+z^2\\(2y-3z)^2+(y+6z)^2+z^2\end{cases}$ |
| $169+36+25$<br>$196+25+9$ | $11y^2+20yz+30z^2=\begin{cases}(3y+2z)^2+(y+5z)^2+(y-z)^2\\(3y+z)^2+(y+5z)^2+(y+2z)^2\end{cases}$ |
| $100+81+49$<br>$121+100+9$ | $19y^2+12yz+14z^2=\begin{cases}(3y+2z)^2+(3y-z)^2+(y+3z)^2\\(3y+2z)^2+(3y+z)^2+(y-3z)^2\end{cases}$ |
| | $\left.\begin{matrix}2y^2+115z^2\\3y^2+4yz+78z^2\\18y^2+4yz+13z^2\end{matrix}\right\}$ *non décomposables.* |
| | $t^2 + 238u^2$ |
| $121+81+36$<br>$225+9+4$ | $13y^2+20yz+26z^2=\begin{cases}(3y+4z)^2+(2y-z)^2+9z^2\\(2y+5z)^2+9y^2+z^2\end{cases}$ |
| | $11y^2+4yz+22z^2$ *non décomposable.* |
| | $t^2 + 246u^2$ |
| $121+121+4$<br>$196+25+25$ | $2y^2+123z^2=\begin{cases}(y+z)^2+(y-z)^2+121z^2\\(y+7z)^2+(y-7z)^2+25z^2\end{cases}$ |
| $196+49+1$<br>$121+100+25$ | $5y^2+4yz+50z^2=\begin{cases}(2y+z)^2+y^2+49z^2\\(2y+3z)^2+(y-4z)^2+25z^2\end{cases}$ |
| | $\left.\begin{matrix}3y^2+82z^2\\13y^2+24yz+30z^2\end{matrix}\right\}$ *non décomposables.* |

TABLE XII.

# TABLE XII.

FRACTIONS les plus simples $\frac{m}{n}$ qui satisfont à l'équation $m^2 - a n^2 = \pm 1$, pour tout nombre non quarré $a$ depuis 2 jusqu'à 1003.

| N. | FRACT. | N. | FRACT. | N. | FRACT. | N. | FRACT. |
|---|---|---|---|---|---|---|---|
| 2 | $\frac{1}{1}$ | 39 | $\frac{25}{4}$ | 73 | $\frac{1068}{125}$ | 107 | $\frac{962}{93}$ |
| 3 | $\frac{2}{1}$ | 40 | $\frac{19}{3}$ | 74 | $\frac{43}{5}$ | 108 | $\frac{1351}{130}$ |
| 5 | $\frac{2}{1}$ | 41 | $\frac{32}{5}$ | 75 | $\frac{26}{3}$ | 109 | $\frac{8890182}{851525}$ |
| 6 | $\frac{5}{2}$ | 42 | $\frac{13}{2}$ | 76 | $\frac{57799}{6630}$ | 110 | $\frac{21}{2}$ |
| 7 | $\frac{8}{3}$ | 43 | $\frac{3482}{531}$ | 77 | $\frac{351}{40}$ | 111 | $\frac{295}{28}$ |
| 8 | $\frac{3}{1}$ | 44 | $\frac{199}{30}$ | 78 | $\frac{53}{6}$ | 112 | $\frac{127}{12}$ |
| 10 | $\frac{3}{1}$ | 45 | $\frac{161}{24}$ | 79 | $\frac{80}{9}$ | 113 | $\frac{776}{73}$ |
| 11 | $\frac{10}{3}$ | 46 | $\frac{24335}{3588}$ | 80 | $\frac{9}{1}$ | 114 | $\frac{1025}{96}$ |
| 12 | $\frac{7}{2}$ | 47 | $\frac{48}{7}$ | 82 | $\frac{9}{1}$ | 115 | $\frac{1126}{105}$ |
| 13 | $\frac{18}{5}$ | 48 | $\frac{7}{1}$ | 83 | $\frac{82}{9}$ | 116 | $\frac{9801}{910}$ |
| 14 | $\frac{15}{4}$ | 50 | $\frac{7}{1}$ | 84 | $\frac{55}{6}$ | 117 | $\frac{649}{60}$ |
| 15 | $\frac{4}{1}$ | 51 | $\frac{50}{7}$ | 85 | $\frac{378}{41}$ | 118 | $\frac{306917}{28254}$ |
| 17 | $\frac{4}{1}$ | 52 | $\frac{649}{90}$ | 86 | $\frac{10405}{1122}$ | 119 | $\frac{120}{11}$ |
| 18 | $\frac{17}{4}$ | 53 | $\frac{182}{25}$ | 87 | $\frac{28}{3}$ | 120 | $\frac{11}{1}$ |
| 19 | $\frac{170}{39}$ | 54 | $\frac{485}{66}$ | 88 | $\frac{197}{21}$ | 122 | $\frac{11}{1}$ |
| 20 | $\frac{9}{2}$ | 55 | $\frac{89}{12}$ | 89 | $\frac{500}{53}$ | 123 | $\frac{122}{11}$ |
| 21 | $\frac{55}{12}$ | 56 | $\frac{15}{2}$ | 90 | $\frac{19}{2}$ | 124 | $\frac{4620799}{414960}$ |
| 22 | $\frac{197}{42}$ | 57 | $\frac{151}{20}$ | 91 | $\frac{1574}{165}$ | 125 | $\frac{682}{61}$ |
| 23 | $\frac{24}{5}$ | 58 | $\frac{99}{13}$ | 92 | $\frac{1151}{120}$ | 126 | $\frac{449}{40}$ |
| 24 | $\frac{5}{1}$ | 59 | $\frac{530}{69}$ | 93 | $\frac{12151}{1260}$ | 127 | $\frac{4730624}{419775}$ |
| 26 | $\frac{5}{1}$ | 60 | $\frac{31}{4}$ | 94 | $\frac{2143295}{221064}$ | 128 | $\frac{577}{51}$ |
| 27 | $\frac{26}{5}$ | 61 | $\frac{29718}{3805}$ | 95 | $\frac{39}{4}$ | 129 | $\frac{16855}{1484}$ |
| 28 | $\frac{127}{24}$ | 62 | $\frac{63}{8}$ | 96 | $\frac{49}{5}$ | 130 | $\frac{57}{5}$ |
| 29 | $\frac{70}{13}$ | 63 | $\frac{8}{1}$ | 97 | $\frac{5604}{569}$ | 131 | $\frac{10610}{927}$ |
| 30 | $\frac{11}{2}$ | 65 | $\frac{8}{1}$ | 98 | $\frac{99}{10}$ | 132 | $\frac{23}{2}$ |
| 31 | $\frac{1520}{273}$ | 66 | $\frac{65}{8}$ | 99 | $\frac{10}{1}$ | 133 | $\frac{2588599}{224460}$ |
| 32 | $\frac{17}{3}$ | 67 | $\frac{48842}{5967}$ | 101 | $\frac{10}{1}$ | 134 | $\frac{145925}{12606}$ |
| 33 | $\frac{23}{4}$ | 68 | $\frac{33}{4}$ | 102 | $\frac{101}{10}$ | 135 | $\frac{244}{21}$ |
| 34 | $\frac{35}{6}$ | 69 | $\frac{7775}{936}$ | 103 | $\frac{227528}{22419}$ | 136 | $\frac{35}{3}$ |
| 35 | $\frac{6}{1}$ | 70 | $\frac{251}{30}$ | 104 | $\frac{51}{5}$ | 137 | $\frac{1744}{149}$ |
| 37 | $\frac{6}{1}$ | 71 | $\frac{3480}{413}$ | 105 | $\frac{41}{4}$ | 138 | $\frac{47}{4}$ |
| 38 | $\frac{37}{6}$ | 72 | $\frac{17}{2}$ | 106 | $\frac{4005}{389}$ | 139 | $\frac{77563250}{6578829}$ |

# TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|---|---|
| 140 | $\frac{71}{6}$ | 178 | $\frac{1601}{120}$ | 215 | $\frac{44}{3}$ |
| 141 | $\frac{95}{8}$ | 179 | $\frac{4190210}{313191}$ | 216 | $\frac{485}{33}$ |
| 142 | $\frac{143}{12}$ | 180 | $\frac{161}{12}$ | 217 | $\frac{3844063}{260952}$ |
| 143 | $\frac{12}{1}$ | 181 | $\frac{1111225770}{82596761}$ | 218 | $\frac{251}{17}$ |
| 145 | $\frac{12}{1}$ | 182 | $\frac{27}{2}$ | 219 | $\frac{74}{5}$ |
| 146 | $\frac{145}{12}$ | 183 | $\frac{487}{36}$ | 220 | $\frac{89}{6}$ |
| 147 | $\frac{97}{8}$ | 184 | $\frac{24335}{1794}$ | 221 | $\frac{1665}{112}$ |
| 148 | $\frac{73}{6}$ | 185 | $\frac{68}{5}$ | 222 | $\frac{149}{10}$ |
| 149 | $\frac{113582}{9305}$ | 186 | $\frac{7501}{550}$ | 223 | $\frac{224}{15}$ |
| 150 | $\frac{49}{4}$ | 187 | $\frac{1682}{123}$ | 224 | $\frac{15}{1}$ |
| 151 | $\frac{1728148040}{140634693}$ | 188 | $\frac{4607}{336}$ | 226 | $\frac{15}{1}$ |
| 152 | $\frac{37}{3}$ | 189 | $\frac{55}{4}$ | 227 | $\frac{226}{15}$ |
| 153 | $\frac{2177}{176}$ | 190 | $\frac{52021}{3774}$ | 228 | $\frac{151}{10}$ |
| 154 | $\frac{21295}{1716}$ | 191 | $\frac{8994000}{650783}$ | 229 | $\frac{1710}{113}$ |
| 155 | $\frac{249}{20}$ | 192 | $\frac{97}{7}$ | 230 | $\frac{91}{6}$ |
| 156 | $\frac{25}{2}$ | 193 | $\frac{1764132}{126985}$ | 231 | $\frac{76}{5}$ |
| 157 | $\frac{4852118}{385645}$ | 194 | $\frac{195}{14}$ | 232 | $\frac{19603}{1287}$ |
| 158 | $\frac{7743}{616}$ | 195 | $\frac{14}{1}$ | 233 | $\frac{23156}{1517}$ |
| 159 | $\frac{1324}{105}$ | 197 | $\frac{14}{1}$ | 234 | $\frac{5201}{340}$ |
| 160 | $\frac{721}{57}$ | 198 | $\frac{197}{14}$ | 235 | $\frac{46}{3}$ |
| 161 | $\frac{11775}{928}$ | 199 | $\frac{16266196520}{1153080099}$ | 236 | $\frac{161801}{36570}$ |
| 162 | $\frac{19601}{1540}$ | 200 | $\frac{99}{7}$ | 237 | $\frac{228151}{14820}$ |
| 163 | $\frac{64080026}{5019135}$ | 201 | $\frac{515095}{36332}$ | 238 | $\frac{11663}{756}$ |
| 164 | $\frac{2049}{160}$ | 202 | $\frac{3141}{221}$ | 239 | $\frac{6195120}{400729}$ |
| 165 | $\frac{1079}{84}$ | 203 | $\frac{57}{4}$ | 240 | $\frac{31}{2}$ |
| 166 | $\frac{1700902565}{132015642}$ | 204 | $\frac{4999}{350}$ | 241 | $\frac{71011068}{4574225}$ |
| 167 | $\frac{168}{13}$ | 205 | $\frac{39689}{2772}$ | 242 | $\frac{19601}{1260}$ |
| 168 | $\frac{13}{1}$ | 206 | $\frac{59535}{4148}$ | 243 | $\frac{70226}{4505}$ |
| 170 | $\frac{13}{1}$ | 207 | $\frac{1151}{80}$ | 244 | $\frac{1766319049}{113076990}$ |
| 171 | $\frac{170}{13}$ | 208 | $\frac{649}{45}$ | 245 | $\frac{51841}{3312}$ |
| 172 | $\frac{24248647}{1848942}$ | 209 | $\frac{46551}{3220}$ | 246 | $\frac{88805}{5662}$ |
| 173 | $\frac{1118}{85}$ | 210 | $\frac{29}{2}$ | 247 | $\frac{85292}{5427}$ |
| 174 | $\frac{1451}{110}$ | 211 | $\frac{278354373650}{19162705353}$ | 248 | $\frac{63}{4}$ |
| 175 | $\frac{2024}{153}$ | 212 | $\frac{66249}{4550}$ | 249 | $\frac{8553815}{542076}$ |
| 176 | $\frac{199}{15}$ | 213 | $\frac{194399}{13320}$ | 250 | $\frac{4443}{281}$ |
| 177 | $\frac{62423}{4692}$ | 214 | $\frac{695375867665}{47534345676}$ | 251 | $\frac{3674890}{231957}$ |

## TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|---|---|
| 252 | $\frac{127}{8}$ | 290 | $\frac{17}{1}$ | 327 | $\frac{217}{12}$ |
| 253 | $\frac{3222617399}{202604220}$ | 291 | $\frac{290}{17}$ | 328 | $\frac{163}{9}$ |
| 254 | $\frac{255}{16}$ | 292 | $\frac{2281249}{133500}$ | 329 | $\frac{2376415}{131016}$ |
| 255 | $\frac{16}{1}$ | 293 | $\frac{2482}{145}$ | 330 | $\frac{109}{6}$ |
| 257 | $\frac{16}{1}$ | 294 | $\frac{4801}{280}$ | 331 | $\frac{2785589801443969}{153109862634573}$ |
| 258 | $\frac{257}{16}$ | 295 | $\frac{2024999}{117900}$ | 332 | $\frac{13447}{738}$ |
| 259 | $\frac{847225}{52644}$ | 296 | $\frac{3699}{215}$ | 333 | $\frac{73}{4}$ |
| 260 | $\frac{129}{8}$ | 297 | $\frac{48599}{2820}$ | 334 | $\frac{63804373719695}{3491219999244}$ |
| 261 | $\frac{192119201}{11891880}$ | 298 | $\frac{409557}{23725}$ | 335 | $\frac{604}{33}$ |
| 262 | $\frac{104980517}{6485718}$ | 299 | $\frac{415}{24}$ | 336 | $\frac{55}{3}$ |
| 263 | $\frac{139128}{8579}$ | 300 | $\frac{1351}{78}$ | 337 | $\frac{1015827336}{55331644}$ |
| 264 | $\frac{65}{4}$ | 301 | $\frac{5883392537695}{344299196332}$ | 338 | $\frac{239}{13}$ |
| 265 | $\frac{6072}{373}$ | 302 | $\frac{4276623}{246092}$ | 339 | $\frac{97970}{5321}$ |
| 266 | $\frac{685}{42}$ | 303 | $\frac{2524}{145}$ | 340 | $\frac{285769}{15498}$ |
| 267 | $\frac{2402}{147}$ | 304 | $\frac{57799}{3315}$ | 341 | $\frac{10626551}{575460}$ |
| 268 | $\frac{4771081927}{291440214}$ | 305 | $\frac{489}{28}$ | 342 | $\frac{37}{2}$ |
| 269 | $\frac{82}{5}$ | 306 | $\frac{35}{2}$ | 343 | $\frac{2080149877}{112317136}$ |
| 270 | $\frac{5291}{322}$ | 307 | $\frac{88529282}{5052633}$ | 344 | $\frac{10403}{1122}$ |
| 271 | $\frac{115974983600}{7044978537}$ | 308 | $\frac{351}{20}$ | 345 | $\frac{6761}{364}$ |
| 272 | $\frac{33}{2}$ | 309 | $\frac{6425027125495}{365513363444}$ | 346 | $\frac{93}{5}$ |
| 273 | $\frac{727}{44}$ | 310 | $\frac{848719}{48204}$ | 347 | $\frac{641602}{34443}$ |
| 274 | $\frac{1407}{85}$ | 311 | $\frac{16883880}{957397}$ | 348 | $\frac{1567}{84}$ |
| 275 | $\frac{199}{12}$ | 312 | $\frac{53}{3}$ | 349 | $\frac{9210}{493}$ |
| 276 | $\frac{7775}{468}$ | 313 | $\frac{126862368}{7170685}$ | 350 | $\frac{449}{24}$ |
| 277 | $\frac{8920484118}{535979945}$ | 314 | $\frac{443}{25}$ | 351 | $\frac{62425}{3332}$ |
| 278 | $\frac{2501}{150}$ | 315 | $\frac{71}{4}$ | 352 | $\frac{77617}{4137}$ |
| 279 | $\frac{1520}{91}$ | 316 | $\frac{12799}{720}$ | 353 | $\frac{71264}{3793}$ |
| 280 | $\frac{251}{15}$ | 317 | $\frac{352618}{19805}$ | 354 | $\frac{258065}{13716}$ |
| 281 | $\frac{1063532}{63445}$ | 318 | $\frac{107}{6}$ | 355 | $\frac{954809}{50058}$ |
| 282 | $\frac{2351}{140}$ | 319 | $\frac{12901780}{722366}$ | 356 | $\frac{500001}{26500}$ |
| 283 | $\frac{138274082}{8219541}$ | 320 | $\frac{161}{9}$ | 357 | $\frac{3401}{180}$ |
| 284 | $\frac{24220799}{1437240}$ | 321 | $\frac{215}{12}$ | 358 | $\frac{176579805797}{9332532726}$ |
| 285 | $\frac{2431}{144}$ | 322 | $\frac{323}{18}$ | 359 | $\frac{360}{19}$ |
| 286 | $\frac{561835}{33222}$ | 323 | $\frac{18}{1}$ | 360 | $\frac{19}{1}$ |
| 287 | $\frac{288}{17}$ | 325 | $\frac{18}{1}$ | 362 | $\frac{19}{1}$ |
| 288 | $\frac{17}{1}$ | 326 | $\frac{325}{18}$ | 363 | $\frac{362}{19}$ |

| N. | FRACTIONS. | N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|---|---|
| 364 | 4954951/259710 | 401 | 20/1 | 437 | 4599/220 |
| 365 | 3458/181 | 402 | 401/20 | 438 | 293/14 |
| 366 | 907925/47458 | 403 | 669878/33369 | 439 | 440/21 |
| 367 | 19019995568/992835687 | 404 | 201/10 | 440 | 21/1 |
| 368 | 1151/60 | 405 | 161/8 | 442 | 21/1 |
| 369 | 8396801/437120 | 406 | 59468095/2951352 | 443 | 442/21 |
| 370 | 327/17 | 407 | 2663/132 | 444 | 295/14 |
| 371 | 1695/88 | 408 | 101/5 | 445 | 4662/221 |
| 372 | 12151/630 | 409 | 111921796968/5534176685 | 446 | 110166015/5216512 |
| 373 | 5118/265 | 410 | 81/4 | 447 | 148/7 |
| 374 | 3365/174 | 411 | 49730/2453 | 448 | 127/6 |
| 375 | 15124/781 | 412 | 103537981567/5100950238 | 449 | 189471332/8941705 |
| 376 | 2143295/110532 | 413 | 113399/5580 | 450 | 19601/924 |
| 377 | 233/12 | 414 | 24335/1196 | 451 | 46471490/2188217 |
| 378 | 8749/450 | 415 | 18412804/903847 | 452 | 1204353/56648 |
| 379 | 12941197220540690/664744650125541 | 416 | 5201/255 | 453 | 1653751/77700 |
| 380 | 39/2 | 417 | 85322647/4178268 | 454 | 16916044084175685/793909098494766 |
| 381 | 1015/52 | 418 | 33857/1656 | 455 | 64/3 |
| 382 | 164998439999/8442054600 | 419 | 270174970/13198911 | 456 | 1025/48 |
| 383 | 18768/959 | 420 | 41/2 | 457 | 59089951584/2764111349 |
| 384 | 4801/245 | 421 | 440424445696821418/21464974635530785 | 458 | 107/5 |
| 385 | 95831/4884 | 422 | 7022501/341850 | 459 | 499850/23331 |
| 386 | 111555/5678 | 423 | 4607/224 | 460 | 2535751/118230 |
| 387 | 3482/177 | 424 | 32080051/1557945 | 461 | 24514110/1134421 |
| 388 | 62809633/3188676 | 425 | 268/13 | 462 | 43/2 |
| 389 | 1282/65 | 426 | 88751/4300 | 463 | 247512720456568/11502891625161 |
| 390 | 79/4 | 427 | 62/3 | 464 | 9801/455 |
| 391 | 7338680/371133 | 428 | 1850887/89466 | 465 | 15871/736 |
| 392 | 99/5 | 429 | 1524095/73584 | 466 | 958519425/03466808 |
| 393 | 46437143/2342444 | 430 | 2862251/138030 | 467 | 1625626/75225 |
| 394 | 395023035/19900973 | 431 | 151560720/7300423 | 468 | 649/30 |
| 395 | 159/8 | 432 | 1351/65 | 469 | 137815/6336 |
| 396 | 199/10 | 433 | 7230660684/347483377 | 470 | 1691/78 |
| 397 | 20692572243/1047100765 | 434 | 125/6 | 471 | 7838695/361188 |
| 398 | 399/20 | 435 | 146/7 | 472 | 306917/14127 |
| 399 | 20/1 | 436 | 158070671986249/7570212227550 | 473 | 87/4 |

TABLE XII.

# TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|
| 474 | $\frac{193549}{8890}$ | 511 | $\frac{4188548960}{185290497}$ |
| 475 | $\frac{57799}{2652}$ | 512 | $\frac{665857}{29427}$ |
| 476 | $\frac{28799}{1320}$ | 513 | $\frac{13771351}{608020}$ |
| 477 | $\frac{8777860001}{401910600}$ | 514 | $\frac{4625}{204}$ |
| 478 | $\frac{1617319577991743}{73974475657896}$ | 515 | $\frac{17406}{767}$ |
| 479 | $\frac{2989440}{136591}$ | 516 | $\frac{16855}{742}$ |
| 480 | $\frac{241}{11}$ | 517 | $\frac{590968951399}{25990786260}$ |
| 481 | $\frac{964140}{43961}$ | 518 | $\frac{2367}{104}$ |
| 482 | $\frac{483}{22}$ | 519 | $\frac{14851876}{651925}$ |
| 483 | $\frac{22}{1}$ | 520 | $\frac{6499}{285}$ |
| 485 | $\frac{22}{1}$ | 521 | $\frac{128377240}{5624309}$ |
| 486 | $\frac{485}{22}$ | 522 | $\frac{19603}{858}$ |
| 487 | $\frac{51906073840568}{2352088722477}$ | 523 | $\frac{81810300626}{3577314675}$ |
| 488 | $\frac{243}{11}$ | 524 | $\frac{225144199}{9835470}$ |
| 489 | $\frac{7592629975}{343350596}$ | 525 | $\frac{6049}{264}$ |
| 490 | $\frac{1039681}{46968}$ | 526 | $\frac{84086091456952913771}{3666119767224284532}$ |
| 491 | $\frac{93628044170}{4225374483}$ | 527 | $\frac{528}{23}$ |
| 492 | $\frac{29767}{1342}$ | 528 | $\frac{23}{1}$ |
| 493 | $\frac{683980}{30805}$ | 530 | $\frac{23}{1}$ |
| 494 | $\frac{75035}{3376}$ | 531 | $\frac{530}{23}$ |
| 495 | $\frac{89}{4}$ | 532 | $\frac{2588599}{112230}$ |
| 496 | $\frac{4620799}{207480}$ | 533 | $\frac{6118}{265}$ |
| 497 | $\frac{1201887}{53912}$ | 534 | $\frac{3678725}{159194}$ |
| 498 | $\frac{179777}{8056}$ | 535 | $\frac{1618804}{69987}$ |
| 499 | $\frac{4490}{201}$ | 536 | $\frac{145925}{6303}$ |
| 500 | $\frac{930249}{41602}$ | 537 | $\frac{192349463}{8300492}$ |
| 501 | $\frac{11242731900975}{502288218432}$ | 538 | $\frac{69051}{2977}$ |
| 502 | $\frac{3832352837}{171046278}$ | 539 | $\frac{3970}{171}$ |
| 503 | $\frac{24648}{1099}$ | 540 | $\frac{119071}{5124}$ |
| 504 | $\frac{449}{20}$ | 541 | $\frac{1361516316469117457}{58536158470221581}$ |
| 505 | $\frac{809}{36}$ | 542 | $\frac{4293183}{184408}$ |
| 506 | $\frac{45}{2}$ | 543 | $\frac{669337}{28724}$ |
| 507 | $\frac{1351}{60}$ | 544 | $\frac{2449}{105}$ |
| 508 | $\frac{44757606858751}{1985797689600}$ | 545 | $\frac{1961}{84}$ |
| 509 | $\frac{3957727950}{175403335}$ | 546 | $\frac{701}{30}$ |
| 510 | $\frac{271}{12}$ | 547 | $\frac{160177601164642}{6848699678675}$ |

# TABLE XI.

| NOMBRE $2a$. | DIVISEURS $8n+3, 8n+5$. |
|---|---|
| | $t^2 + 126u^2$ |
| $121+4+1$<br>$100+25+1$<br>$81+36+9$ | $5y^2+4yz+26z^2=\begin{cases}(y-4z)^2+(2y+3z)^2+z^2\\ y^2+(2y+z)^2+25z^2\\ (2y-z)^2+(y+4z)^2+9z^2\end{cases}$ |
| | $\left.\begin{matrix}3y^2+42z^2\\ 6y^2+21z^2\end{matrix}\right\}$ *non décomposables.* |
| $81+36+9$ | $10y^2+4yz+13z^2=9y^2+(y+2z)^2+9z^2$ |
| | $t^2 + 134u^2$ |
| $49+49+36$<br>$121+9+4$<br>$100+25+9$<br>$81+49+4$ | $2y^2+67z^2=(y+3z)^2+(y-3z)^2+49z^2$<br>$11y^2+16yz+18z^2=(3y+z)^2+(y+4z)^2+(y+z)^2$<br>$5y^2+8yz+30z^2=(y+2z)^2+(2y+z)^2+25z^2$<br>$3y^2+4yz+46z^2=(y-z)^2+(y+6z)^2+(y-3z)^2$ |
| | $t^2 + 142u^2$ |
| $81+36+25$ | $11y^2+20yz+22z^2=(3y+3z)^2+(y+3z)^2+(y-2z)^2$ |
| | $t^2 + 150u^2$ |
| $121+25+4$<br>$100+49+1$<br>$100+25+25$ | $11y^2+4yz+14z^2=\begin{cases}(3y+2z)^2+(y-z)^2+(y-3z)^2\\ (3y-z)^2+(y+3z)^2+(y+2z)^2\\ (3y+z)^2+(y-3z)^2+(y+2z)^2\end{cases}$ |
| $100+25+25$<br>$100+25+25$<br>$100+25+25$ | $2y^2+75z^2=(y+5z)^2+(y-5z)^2+25z^2$<br>$3y^2+50z^2=(y+5z)^2+(y-5z)^2+y^2$<br>$5y^2+30z^2=(2y+z)^2+(y-2z)^2+25z^2$ |
| | $t^2 + 158u^2$ |
| $100+49+9$<br>$121+36+1$ | $3y^2+4yz+54z^2=(y+5z)^2+(y-5z)^2+(y+2z)^2$<br>$6y^2+4yz+27z^2=(2y-z)^2+(y+5z)^2+(y-z)^2$ |
| | $t^2 + 166u^2$ |
| $81+81+4$<br>$121+36+9$<br>$81+49+36$ | $2y^2+83z^2=(y+z)^2+(y-z)^2+81z^2$<br>$5y^2+4yz+34z^2=(2y+3z)^2+(y-4z)^2+9z^2$<br>$13y^2+8yz+14z^2=(3y+2z)^2+(2y-z)^2+9z^2$ |

# TABLE XI.

| NOMBRE 2 *a*. | DIVISEURS $8n+3$, $8n+5$. |
|---|---|
| | $t^2 + 174u^2$ |
| 121+49+4 | $6y^2+29z^2 = \begin{cases}(y-4z)^2+(2y+3z)^2+(y-2z)^2\\(y+4z)^2+(2y-3z)^2+(y+2z)^2\end{cases}$ |
| 100+49+25<br>169+4+1 | $5y^2+8yz+38z^2 = \begin{cases}(2y+3z)^2+(y-2z)^2+25z^2\\(2y-z)^2+(y+6z)^2+z^2\end{cases}$ |
| | $\left.\begin{matrix}3y^2+58z^2\\10y^2+8yz+19z^2\end{matrix}\right\}$ *non décomposables.* |
| | $t^2 + 182u^2$ |
| 169+9+4 | $13y^2+14z^2 = \begin{cases}(3y+2z)^2+(2y-3z)^2+z^2\\(3y-2z)^2+(2y+3z)^2+z^2\end{cases}$ |
| 100+81+1<br>121+36+25 | $3y^2+4yz+62z^2 = \begin{cases}(y+7z)^2+(y-3z)^2+(y-2z)^2\\(y+6z)^2+(y-5z)^2+(y+z)^2\end{cases}$ |
| | $2y^2+91z^2$ *non décomposable.* |
| | $t^2 + 190u^2$ |
| 100+81+9 | $10y^2+19z^2 = \begin{cases}(3y+z)^2+(y-3z)^2+9z^2\\(3y-z)^2+(y+3z)^2+9z^2\end{cases}$ |
| | $5y^2+38z^2$ *non décomposable.* |
| | $t^2 + 198u^2$ |
| 196+1+1<br>100+49+49<br>81+81+36 | $2y^2+99z^2 = \begin{cases}(y+7z)^2+(y-7z)^2+z^2\\(y+5z)^2+(y-5z)^2+49z^2\\(y+3z)^2+(y-3z)^2+81z^2\end{cases}$ |
| | $3y^2+66z^2$ *non décomposable.* |
| 81+81+36<br>81+81+36 | $13y^2+12yz+18z^2=9y^2+9z^2+(2y+3z)^2$<br>$11y^2+18z^2=(y+3z)^2+(y-3z)^2+9y^2$ |
| | $t^2 + 206u^2$ |
| 121+81+4<br>169+36+1<br>100+81+25<br>196+9+1<br>121+49+36 | $3y^2+4yz+70z^2=(y+5z)^2+(y+3z)^2+(y-6z)^2$<br>$6y^2+4yz+35z^2=(2y+3z)^2+(y+z)^2+(y-5z)^2$<br>$5y^2+4yz+42z^2=(2y-z)^2+(y+4z)^2+25z^2$<br>$10y^2+4yz+21z^2=(3y+2z)^2+(y-4z)^2+z^2$<br>$11y^2+12yz+22z^2=(3y+2z)^2+(y-3z)^2+(y+3z)^2$ |

## TABLE XI.

| NOMBRE $2a$. | DIVISEURS $8n+3,\ 8n+5$. |
|---|---|
| | $t^2+214u^2$ |
| 196+9+9 | $2y^2+107z^2=(y+7z)^2+(y-7z)^2+9z^2$ |
| 169+36+9 | $5y^2+8yz+46z^2=(2y-z)^2+(y+6z)^2+9z^2$ |
| | $t^2+222u^2$ |
| 121+100+1 | $3y^2+74z^2=\begin{cases}(y-7z)^2+(y+4z)^2+(y+3z)^2\\(y+7z)^2+(y-4z)^2+(y-3z)^2\end{cases}$ |
| 196+25+1<br>169+49+4 | $11y^2+16yz+26z^2=\begin{cases}(3y+z)^2+(y+5z)^2+y^2\\(3y+4z)^2+(y-3z)^2+(y-z)^2\end{cases}$ |
| | $\left.\begin{array}{l}6y^2+37z^2\\22y^2+16yz+13z^2\end{array}\right\}$ *non décomposables.* |
| | $t^2+230u^2$ |
| 225+4+1 | $5y^2+46z^2=\begin{cases}(2y+3z)^2+(y-6z)^2+z^2\\(2y-3z)^2+(y+6z)^2+z^2\end{cases}$ |
| 169+36+25<br>196+25+9 | $11y^2+20yz+30z^2=\begin{cases}(3y+2z)^2+(y+5z)^2+(y-z)^2\\(3y+z)^2+(y+5z)^2+(y+2z)^2\end{cases}$ |
| 100+81+49<br>121+100+9 | $19y^2+12yz+14z^2=\begin{cases}(3y+2z)^2+(3y-z)^2+(y+3z)^2\\(3y+2z)^2+(3y+z)^2+(y-3z)^2\end{cases}$ |
| | $\left.\begin{array}{l}2y^2+115z^2\\3y^2+4yz+78z^2\\18y^2+4yz+13z^2\end{array}\right\}$ *non décomposables.* |
| | $t^2+238u^2$ |
| 121+81+36<br>225+9+4 | $13y^2+20yz+26z^2=\begin{cases}(3y+4z)^2+(2y-z)^2+9z^2\\(2y+5z)^2+9y^2+z^2\end{cases}$ |
| | $11y^2+4yz+22z^2$ *non décomposable.* |
| | $t^2+246u^2$ |
| 121+121+4<br>196+25+25 | $2y^2+123z^2=\begin{cases}(y+z)^2+(y-z)^2+121z^2\\(y+7z)^2+(y-7z)^2+25z^2\end{cases}$ |
| 196+49+1<br>121+100+25 | $5y^2+4yz+50z^2=\begin{cases}(2y+z)^2+y^2+49z^2\\(2y+3z)^2+(y-4z)^2+25z^2\end{cases}$ |
| | $\left.\begin{array}{l}3y^2+82z^2\\13y^2+24yz+30z^2\end{array}\right\}$ *non décomposables.* |

# TABLE XII.

FRACTIONS les plus simples $\frac{m}{n}$ qui satisfont à l'équation $m^2 - an^2 = \pm 1$, pour tout nombre non quarré $a$ depuis 2 jusqu'à 1003.

| N. | FRACT. | N. | FRACT. | N. | FRACT. | N. | FRACT. |
|---|---|---|---|---|---|---|---|
| 2 | $\frac{1}{1}$ | 39 | $\frac{25}{4}$ | 73 | $\frac{1068}{125}$ | 107 | $\frac{962}{93}$ |
| 3 | $\frac{2}{1}$ | 40 | $\frac{19}{3}$ | 74 | $\frac{43}{5}$ | 108 | $\frac{1351}{130}$ |
| 5 | $\frac{2}{1}$ | 41 | $\frac{32}{5}$ | 75 | $\frac{26}{3}$ | 109 | $\frac{8890182}{851525}$ |
| 6 | $\frac{5}{2}$ | 42 | $\frac{13}{2}$ | 76 | $\frac{57799}{6630}$ | 110 | $\frac{21}{2}$ |
| 7 | $\frac{8}{3}$ | 43 | $\frac{3482}{531}$ | 77 | $\frac{351}{40}$ | 111 | $\frac{295}{28}$ |
| 8 | $\frac{3}{1}$ | 44 | $\frac{199}{30}$ | 78 | $\frac{53}{6}$ | 112 | $\frac{127}{12}$ |
| 10 | $\frac{3}{1}$ | 45 | $\frac{161}{24}$ | 79 | $\frac{80}{9}$ | 113 | $\frac{776}{73}$ |
| 11 | $\frac{10}{3}$ | 46 | $\frac{24335}{3588}$ | 80 | $\frac{9}{1}$ | 114 | $\frac{1025}{96}$ |
| 12 | $\frac{7}{2}$ | 47 | $\frac{48}{7}$ | 82 | $\frac{9}{1}$ | 115 | $\frac{1126}{105}$ |
| 13 | $\frac{18}{5}$ | 48 | $\frac{7}{1}$ | 83 | $\frac{82}{9}$ | 116 | $\frac{9801}{910}$ |
| 14 | $\frac{15}{4}$ | 50 | $\frac{7}{1}$ | 84 | $\frac{55}{6}$ | 117 | $\frac{649}{60}$ |
| 15 | $\frac{4}{1}$ | 51 | $\frac{50}{7}$ | 85 | $\frac{378}{41}$ | 118 | $\frac{306917}{28254}$ |
| 17 | $\frac{4}{1}$ | 52 | $\frac{649}{90}$ | 86 | $\frac{10405}{1122}$ | 119 | $\frac{120}{11}$ |
| 18 | $\frac{17}{4}$ | 53 | $\frac{182}{25}$ | 87 | $\frac{28}{3}$ | 120 | $\frac{11}{1}$ |
| 19 | $\frac{170}{39}$ | 54 | $\frac{485}{66}$ | 88 | $\frac{197}{21}$ | 122 | $\frac{11}{1}$ |
| 20 | $\frac{9}{2}$ | 55 | $\frac{89}{12}$ | 89 | $\frac{500}{53}$ | 123 | $\frac{122}{11}$ |
| 21 | $\frac{55}{12}$ | 56 | $\frac{15}{2}$ | 90 | $\frac{19}{2}$ | 124 | $\frac{4620799}{414960}$ |
| 22 | $\frac{197}{42}$ | 57 | $\frac{151}{20}$ | 91 | $\frac{1574}{165}$ | 125 | $\frac{682}{61}$ |
| 23 | $\frac{24}{5}$ | 58 | $\frac{99}{13}$ | 92 | $\frac{1151}{120}$ | 126 | $\frac{449}{40}$ |
| 24 | $\frac{5}{1}$ | 59 | $\frac{530}{69}$ | 93 | $\frac{12151}{1260}$ | 127 | $\frac{4730624}{419775}$ |
| 26 | $\frac{5}{1}$ | 60 | $\frac{31}{4}$ | 94 | $\frac{2143295}{221064}$ | 128 | $\frac{577}{51}$ |
| 27 | $\frac{26}{5}$ | 61 | $\frac{29718}{3805}$ | 95 | $\frac{39}{4}$ | 129 | $\frac{16855}{1484}$ |
| 28 | $\frac{127}{24}$ | 62 | $\frac{63}{8}$ | 96 | $\frac{49}{5}$ | 130 | $\frac{57}{5}$ |
| 29 | $\frac{70}{13}$ | 63 | $\frac{8}{1}$ | 97 | $\frac{5604}{569}$ | 131 | $\frac{10610}{927}$ |
| 30 | $\frac{11}{2}$ | 65 | $\frac{8}{1}$ | 98 | $\frac{99}{10}$ | 132 | $\frac{23}{2}$ |
| 31 | $\frac{1520}{273}$ | 66 | $\frac{65}{8}$ | 99 | $\frac{10}{1}$ | 133 | $\frac{2588599}{224460}$ |
| 32 | $\frac{17}{3}$ | 67 | $\frac{48842}{5967}$ | 101 | $\frac{10}{1}$ | 134 | $\frac{145925}{12606}$ |
| 33 | $\frac{23}{4}$ | 68 | $\frac{33}{4}$ | 102 | $\frac{101}{10}$ | 135 | $\frac{244}{21}$ |
| 34 | $\frac{35}{6}$ | 69 | $\frac{7775}{936}$ | 103 | $\frac{227528}{22419}$ | 136 | $\frac{35}{3}$ |
| 35 | $\frac{6}{1}$ | 70 | $\frac{251}{30}$ | 104 | $\frac{51}{5}$ | 137 | $\frac{1744}{149}$ |
| 37 | $\frac{6}{1}$ | 71 | $\frac{3480}{413}$ | 105 | $\frac{41}{4}$ | 138 | $\frac{47}{4}$ |
| 38 | $\frac{37}{6}$ | 72 | $\frac{17}{2}$ | 106 | $\frac{4005}{389}$ | 139 | $\frac{77563250}{6578829}$ |

# TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|---|---|
| 140 | $\frac{71}{6}$ | 178 | $\frac{1601}{120}$ | 215 | $\frac{44}{3}$ |
| 141 | $\frac{95}{8}$ | 179 | $\frac{4190210}{313191}$ | 216 | $\frac{485}{33}$ |
| 142 | $\frac{143}{12}$ | 180 | $\frac{161}{12}$ | 217 | $\frac{3844063}{260952}$ |
| 143 | $\frac{12}{1}$ | 181 | $\frac{1111225770}{82596761}$ | 218 | $\frac{251}{17}$ |
| 145 | $\frac{12}{1}$ | 182 | $\frac{27}{2}$ | 219 | $\frac{74}{5}$ |
| 146 | $\frac{145}{12}$ | 183 | $\frac{487}{36}$ | 220 | $\frac{89}{6}$ |
| 147 | $\frac{97}{8}$ | 184 | $\frac{24335}{1794}$ | 221 | $\frac{1665}{112}$ |
| 148 | $\frac{73}{6}$ | 185 | $\frac{68}{5}$ | 222 | $\frac{149}{10}$ |
| 149 | $\frac{113582}{9305}$ | 186 | $\frac{7501}{550}$ | 223 | $\frac{224}{15}$ |
| 150 | $\frac{49}{4}$ | 187 | $\frac{1682}{123}$ | 224 | $\frac{15}{1}$ |
| 151 | $\frac{1728148040}{140634693}$ | 188 | $\frac{4607}{336}$ | 226 | $\frac{15}{1}$ |
| 152 | $\frac{37}{3}$ | 189 | $\frac{55}{4}$ | 227 | $\frac{226}{15}$ |
| 153 | $\frac{2177}{176}$ | 190 | $\frac{52021}{3774}$ | 228 | $\frac{151}{10}$ |
| 154 | $\frac{21295}{1716}$ | 191 | $\frac{8994000}{650783}$ | 229 | $\frac{1710}{113}$ |
| 155 | $\frac{249}{20}$ | 192 | $\frac{97}{7}$ | 230 | $\frac{91}{6}$ |
| 156 | $\frac{25}{2}$ | 193 | $\frac{1764132}{126985}$ | 231 | $\frac{76}{5}$ |
| 157 | $\frac{4832118}{385645}$ | 194 | $\frac{195}{14}$ | 232 | $\frac{19603}{1287}$ |
| 158 | $\frac{7743}{616}$ | 195 | $\frac{14}{1}$ | 233 | $\frac{23156}{1517}$ |
| 159 | $\frac{1324}{105}$ | 197 | $\frac{14}{1}$ | 234 | $\frac{5201}{340}$ |
| 160 | $\frac{721}{57}$ | 198 | $\frac{197}{14}$ | 235 | $\frac{46}{3}$ |
| 161 | $\frac{11775}{928}$ | 199 | $\frac{16266196520}{1153080099}$ | 236 | $\frac{561801}{36570}$ |
| 162 | $\frac{19601}{1540}$ | 200 | $\frac{99}{7}$ | 237 | $\frac{228151}{14820}$ |
| 163 | $\frac{64080026}{5019135}$ | 201 | $\frac{515095}{36332}$ | 238 | $\frac{11663}{756}$ |
| 164 | $\frac{2049}{160}$ | 202 | $\frac{3141}{221}$ | 239 | $\frac{6195120}{400729}$ |
| 165 | $\frac{1079}{84}$ | 203 | $\frac{57}{4}$ | 240 | $\frac{31}{2}$ |
| 166 | $\frac{1700902565}{132015642}$ | 204 | $\frac{4999}{350}$ | 241 | $\frac{71011068}{4574225}$ |
| 167 | $\frac{168}{13}$ | 205 | $\frac{39689}{2772}$ | 242 | $\frac{19601}{1260}$ |
| 168 | $\frac{13}{1}$ | 206 | $\frac{59535}{4148}$ | 243 | $\frac{70226}{4505}$ |
| 170 | $\frac{13}{1}$ | 207 | $\frac{1151}{80}$ | 244 | $\frac{1766319049}{113076990}$ |
| 171 | $\frac{170}{13}$ | 208 | $\frac{649}{45}$ | 245 | $\frac{51841}{3312}$ |
| 172 | $\frac{24248647}{1848942}$ | 209 | $\frac{46551}{3220}$ | 246 | $\frac{88805}{5662}$ |
| 173 | $\frac{1118}{85}$ | 210 | $\frac{29}{2}$ | 247 | $\frac{85292}{5427}$ |
| 174 | $\frac{1451}{110}$ | 211 | $\frac{278354373650}{19162705353}$ | 248 | $\frac{63}{4}$ |
| 175 | $\frac{2024}{153}$ | 212 | $\frac{66249}{4550}$ | 249 | $\frac{8553815}{542076}$ |
| 176 | $\frac{199}{15}$ | 213 | $\frac{194399}{13320}$ | 250 | $\frac{4443}{281}$ |
| 177 | $\frac{62423}{4692}$ | 214 | $\frac{695375847665}{47534345676}$ | 251 | $\frac{3674890}{231957}$ |

# TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|---|---|
| 252 | $\frac{127}{8}$ | 290 | $\frac{17}{1}$ | 327 | $\frac{217}{12}$ |
| 253 | $\frac{3222617199}{202604220}$ | 291 | $\frac{290}{17}$ | 328 | $\frac{163}{9}$ |
| 254 | $\frac{255}{16}$ | 292 | $\frac{2281249}{133500}$ | 329 | $\frac{2376415}{131016}$ |
| 255 | $\frac{16}{1}$ | 293 | $\frac{2482}{145}$ | 330 | $\frac{109}{6}$ |
| 257 | $\frac{16}{1}$ | 294 | $\frac{4801}{280}$ | 331 | $\frac{2785589801443969}{153109862634573}$ |
| 258 | $\frac{257}{16}$ | 295 | $\frac{2024999}{117900}$ | 332 | $\frac{13447}{738}$ |
| 259 | $\frac{847225}{52644}$ | 296 | $\frac{3699}{215}$ | 333 | $\frac{73}{4}$ |
| 260 | $\frac{129}{8}$ | 297 | $\frac{48599}{2820}$ | 334 | $\frac{638043737219695}{34912219999244}$ |
| 261 | $\frac{1925119201}{119161880}$ | 298 | $\frac{409557}{23725}$ | 335 | $\frac{604}{33}$ |
| 262 | $\frac{104980517}{6485718}$ | 299 | $\frac{415}{24}$ | 336 | $\frac{55}{3}$ |
| 263 | $\frac{139128}{8579}$ | 300 | $\frac{1351}{78}$ | 337 | $\frac{10155827336}{553231641}$ |
| 264 | $\frac{65}{4}$ | 301 | $\frac{58833925537695}{3442999196232}$ | 338 | $\frac{239}{13}$ |
| 265 | $\frac{6072}{373}$ | 302 | $\frac{4276623}{246092}$ | 339 | $\frac{97970}{5321}$ |
| 266 | $\frac{685}{42}$ | 303 | $\frac{2524}{145}$ | 340 | $\frac{285769}{15498}$ |
| 267 | $\frac{2402}{147}$ | 304 | $\frac{57799}{3315}$ | 341 | $\frac{10626551}{575460}$ |
| 268 | $\frac{4771081927}{291440214}$ | 305 | $\frac{489}{28}$ | 342 | $\frac{37}{2}$ |
| 269 | $\frac{82}{5}$ | 306 | $\frac{35}{2}$ | 343 | $\frac{2080149577}{112317536}$ |
| 270 | $\frac{5291}{322}$ | 307 | $\frac{88529282}{5052633}$ | 344 | $\frac{10405}{561}$ |
| 271 | $\frac{115974983600}{7044978537}$ | 308 | $\frac{351}{20}$ | 345 | $\frac{6761}{364}$ |
| 272 | $\frac{33}{2}$ | 309 | $\frac{642022723495}{36523365444}$ | 346 | $\frac{93}{5}$ |
| 273 | $\frac{727}{44}$ | 310 | $\frac{848719}{48204}$ | 347 | $\frac{641602}{34443}$ |
| 274 | $\frac{1407}{85}$ | 311 | $\frac{16883880}{957397}$ | 348 | $\frac{1567}{84}$ |
| 275 | $\frac{199}{12}$ | 312 | $\frac{53}{3}$ | 349 | $\frac{9210}{493}$ |
| 276 | $\frac{7775}{468}$ | 313 | $\frac{126862368}{7170685}$ | 350 | $\frac{449}{24}$ |
| 277 | $\frac{8920484118}{535979943}$ | 314 | $\frac{443}{25}$ | 351 | $\frac{62425}{3332}$ |
| 278 | $\frac{2501}{150}$ | 315 | $\frac{71}{4}$ | 352 | $\frac{77617}{4137}$ |
| 279 | $\frac{1520}{91}$ | 316 | $\frac{12799}{720}$ | 353 | $\frac{71264}{3793}$ |
| 280 | $\frac{251}{15}$ | 317 | $\frac{352618}{19805}$ | 354 | $\frac{258065}{13716}$ |
| 281 | $\frac{1063532}{63445}$ | 318 | $\frac{107}{6}$ | 355 | $\frac{954809}{50676}$ |
| 282 | $\frac{2351}{140}$ | 319 | $\frac{12901780}{722361}$ | 356 | $\frac{500001}{26500}$ |
| 283 | $\frac{138274082}{8219541}$ | 320 | $\frac{161}{9}$ | 357 | $\frac{3401}{180}$ |
| 284 | $\frac{24220799}{1437240}$ | 321 | $\frac{215}{12}$ | 358 | $\frac{1765579805799}{93321532726}$ |
| 285 | $\frac{2431}{144}$ | 322 | $\frac{323}{18}$ | 359 | $\frac{360}{19}$ |
| 286 | $\frac{561835}{33222}$ | 323 | $\frac{18}{1}$ | 360 | $\frac{19}{1}$ |
| 287 | $\frac{288}{17}$ | 325 | $\frac{18}{1}$ | 362 | $\frac{19}{1}$ |
| 288 | $\frac{17}{1}$ | 326 | $\frac{325}{18}$ | 363 | $\frac{362}{19}$ |

| N. | FRACTIONS. | N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|---|---|
| 364 | 4954951/259710 | 401 | 20/1 | 437 | 4599/220 |
| 365 | 3458/181 | 402 | 401/20 | 438 | 293/14 |
| 366 | 907925/47458 | 403 | 669878/33369 | 439 | 440/21 |
| 367 | 19019995568/992835687 | 404 | 201/10 | 440 | 21/1 |
| 368 | 1151/60 | 405 | 161/8 | 442 | 21/1 |
| 369 | 8396801/437120 | 406 | 59468095/2951352 | 443 | 442/21 |
| 370 | 327/17 | 407 | 2663/132 | 444 | 295/14 |
| 371 | 1695/88 | 408 | 101/5 | 445 | 4662/221 |
| 372 | 12151/630 | 409 | 111921796968/5534176685 | 446 | 110166015/5216510 |
| 373 | 5118/265 | 410 | 81/4 | 447 | 148/7 |
| 374 | 3365/174 | 411 | 49730/2453 | 448 | 127/6 |
| 375 | 15124/781 | 412 | 103537981567/5100950233 | 449 | 189471332/8941703 |
| 376 | 2143295/110532 | 413 | 113399/5580 | 450 | 19601/924 |
| 377 | 233/12 | 414 | 24335/1196 | 451 | 46471490/2188257 |
| 378 | 8749/450 | 415 | 18412804/903849 | 452 | 1204353/56648 |
| 379 | 12941197230540690/664744650125541 | 416 | 5201/255 | 453 | 1653751/77700 |
| 380 | 39/2 | 417 | 85322647/4178268 | 454 | 16916040084175681/7939707098494766 |
| 381 | 1015/52 | 418 | 33857/1656 | 455 | 64/3 |
| 382 | 164998439999/8442054600 | 419 | 270174970/13198911 | 456 | 1025/48 |
| 383 | 18768/959 | 420 | 41/2 | 457 | 52089951584/2436411349 |
| 384 | 4801/245 | 421 | 44042445696821418/2146497462130785 | 458 | 107/5 |
| 385 | 95831/4884 | 422 | 7022501/341850 | 459 | 499850/23331 |
| 386 | 111555/5678 | 423 | 4607/224 | 460 | 2535751/118230 |
| 387 | 3482/177 | 424 | 32080051/1557945 | 461 | 24514110/1133441 |
| 388 | 62809633/3188676 | 425 | 268/13 | 462 | 43/2 |
| 389 | 1282/65 | 426 | 88751/4300 | 463 | 247512720456168/11502871625161 |
| 390 | 79/4 | 427 | 62/3 | 464 | 9801/455 |
| 391 | 7338680/371133 | 428 | 1850887/89466 | 465 | 15871/736 |
| 392 | 99/5 | 429 | 1524095/73584 | 466 | 938519425/43476808 |
| 393 | 46437148/2342444 | 430 | 2862251/138030 | 467 | 1625626/75225 |
| 394 | 395023035/19900973 | 431 | 151560720/7300423 | 468 | 649/30 |
| 395 | 159/8 | 432 | 1351/65 | 469 | 137215/6336 |
| 396 | 199/10 | 433 | 7230660684/347483377 | 470 | 1691/78 |
| 397 | 206925572242/1047100765 | 434 | 125/6 | 471 | 7838695/361188 |
| 398 | 399/20 | 435 | 146/7 | 472 | 306917/14127 |
| 399 | 20/1 | 436 | 158070471986249/75705112287550 | 473 | 87/4 |

# TABLE XII.

| N. | FRACTIONS. |
|---|---|
| 474 | 193549/8890 |
| 475 | 57799/2652 |
| 476 | 28799/1320 |
| 477 | 8777860001/401910600 |
| 478 | 1617319577991743/73974475657896 |
| 479 | 2989440/136591 |
| 480 | 241/11 |
| 481 | 964140/43961 |
| 482 | 483/22 |
| 483 | 22/1 |
| 485 | 22/1 |
| 486 | 485/22 |
| 487 | 51906073840568/2352088722477 |
| 488 | 243/11 |
| 489 | 7592629979/343350596 |
| 490 | 1039681/46968 |
| 491 | 93628044170/4225374453 |
| 492 | 29767/1342 |
| 493 | 683982/30805 |
| 494 | 73035/3286 |
| 495 | 89/4 |
| 496 | 4620799/207480 |
| 497 | 1201887/53912 |
| 498 | 179777/8056 |
| 499 | 4490/201 |
| 500 | 930249/41602 |
| 501 | 11242731900975/502288218432 |
| 502 | 3832352817/171046278 |
| 503 | 24648/1099 |
| 504 | 449/20 |
| 505 | 809/36 |
| 506 | 45/2 |
| 507 | 1351/60 |
| 508 | 44757606858711/1985797689600 |
| 509 | 395727950/17540335 |
| 510 | 271/12 |
| 511 | 4188545960/185290497 |
| 512 | 665857/29427 |
| 513 | 13771351/608020 |
| 514 | 4625/204 |
| 515 | 17406/767 |
| 516 | 16855/742 |
| 517 | 590968955199/25992786260 |
| 518 | 2367/104 |
| 519 | 148551876/6519235 |
| 520 | 6499/285 |
| 521 | 128377240/5624309 |
| 522 | 19603/858 |
| 523 | 818101300626/35773314671 |
| 524 | 225144199/9835470 |
| 525 | 6049/264 |
| 526 | 841560914156952921775/3666119767224284532 |
| 527 | 528/23 |
| 528 | 23/1 |
| 530 | 23/1 |
| 531 | 530/23 |
| 532 | 2588599/112230 |
| 533 | 6118/265 |
| 534 | 3678725/159194 |
| 535 | 1618804/69987 |
| 536 | 145925/6303 |
| 537 | 192349463/8300492 |
| 538 | 69051/2977 |
| 539 | 3970/171 |
| 540 | 119071/5124 |
| 541 | 1361516316465922725/58536158470221581 |
| 542 | 4293183/184408 |
| 543 | 669337/28724 |
| 544 | 2449/105 |
| 545 | 1961/84 |
| 546 | 701/30 |
| 547 | 160177601264642/6848699678673 |

## TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|
| 548 | $\frac{6083073}{259856}$ | 585 | $\frac{33281}{1376}$ |
| 549 | $\frac{17663190049}{753846660}$ | 586 | $\frac{4115086707}{169992665}$ |
| 550 | $\frac{30580901}{1303974}$ | 587 | $\frac{1907162}{78717}$ |
| 551 | $\frac{8380}{357}$ | 588 | $\frac{97}{4}$ |
| 552 | $\frac{47}{2}$ | 589 | $\frac{41423166067036218711}{1706811823063748000}$ |
| 553 | $\frac{624633837407}{26562217704}$ | 590 | $\frac{5781}{238}$ |
| 554 | $\frac{174293}{7405}$ | 591 | $\frac{165676}{6815}$ |
| 555 | $\frac{1814}{77}$ | 592 | $\frac{73}{3}$ |
| 556 | $\frac{120321115501124999}{510273318434230}$ | 593 | $\frac{600632}{24665}$ |
| 557 | $\frac{118}{5}$ | 594 | $\frac{1098305}{45064}$ |
| 558 | $\frac{7937}{336}$ | 595 | $\frac{18514}{759}$ |
| 559 | $\frac{506568295}{21425556}$ | 596 | $\frac{25801741449}{1056880510}$ |
| 560 | $\frac{71}{3}$ | 597 | $\frac{463287093751}{18961078500}$ |
| 561 | $\frac{522785}{22072}$ | 598 | $\frac{1574351}{64380}$ |
| 562 | $\frac{220938497}{9319728}$ | 599 | $\frac{24686379794520}{1008618133851}$ |
| 563 | $\frac{68122}{2871}$ | 600 | $\frac{49}{2}$ |
| 564 | $\frac{95}{4}$ | 601 | $\frac{139468303679552}{5689030769845}$ |
| 565 | $\frac{14752278}{620633}$ | 602 | $\frac{687}{28}$ |
| 566 | $\frac{95609285}{4018758}$ | 603 | $\frac{48842}{1989}$ |
| 567 | $\frac{2024}{85}$ | 604 | $\frac{59729912963111683199}{243037569063951720}$ |
| 568 | $\frac{143}{6}$ | 605 | $\frac{930249}{37820}$ |
| 569 | $\frac{2894863832}{121359005}$ | 606 | $\frac{42187499}{1713750}$ |
| 570 | $\frac{191}{8}$ | 607 | $\frac{164076013968}{6617640783}$ |
| 571 | $\frac{181124355061630786130}{7579818350828982387}$ | 608 | $\frac{2737}{111}$ |
| 572 | $\frac{287}{12}$ | 609 | $\frac{605695}{24544}$ |
| 573 | $\frac{383}{16}$ | 610 | $\frac{71847}{2909}$ |
| 574 | $\frac{575}{24}$ | 611 | $\frac{236926}{9585}$ |
| 575 | $\frac{24}{1}$ | 612 | $\frac{2177}{88}$ |
| 577 | $\frac{24}{1}$ | 613 | $\frac{482573579088618}{19454612624065}$ |
| 578 | $\frac{577}{24}$ | 614 | $\frac{348291186245}{14055888314}$ |
| 579 | $\frac{385}{16}$ | 615 | $\frac{124}{5}$ |
| 580 | $\frac{289}{12}$ | 616 | $\frac{21295}{858}$ |
| 581 | $\frac{152071113971}{6308974546}$ | 617 | $\frac{41009716}{1650989}$ |
| 582 | $\frac{193}{8}$ | 618 | $\frac{10093}{406}$ |
| 583 | $\frac{8429543}{349116}$ | 619 | $\frac{517213654388408330}{20788569071159439}$ |
| 584 | $\frac{145}{6}$ | 620 | $\frac{249}{10}$ |

# TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|
| 621 | $\frac{7775}{312}$ | 658 | $\frac{1693}{66}$ |
| 622 | $\frac{138043720068}{5535304812}$ | 659 | $\frac{5930}{231}$ |
| 623 | $\frac{624}{25}$ | 660 | $\frac{1079}{42}$ |
| 624 | $\frac{25}{1}$ | 661 | $\frac{2865454435420583218}{111453260376346905}$ |
| 626 | $\frac{25}{1}$ | 662 | $\frac{1718102501}{66775910}$ |
| 627 | $\frac{626}{25}$ | 663 | $\frac{103}{4}$ |
| 628 | $\frac{46698728711849}{1863482146110}$ | 664 | $\frac{1700902565}{66007821}$ |
| 629 | $\frac{8100}{313}$ | 665 | $\frac{13719}{532}$ |
| 630 | $\frac{251}{10}$ | 666 | $\frac{27365201}{1060350}$ |
| 631 | $\frac{48961575312998650055560}{1949129537575151036427}$ | 667 | $\frac{107119097}{4147668}$ |
| 632 | $\frac{7743}{308}$ | 668 | $\frac{56447}{2184}$ |
| 633 | $\frac{440772247}{17519124}$ | 669 | $\frac{14226117859054135}{550013493618436}$ |
| 634 | $\frac{65999458125}{2621171333}$ | 670 | $\frac{5791211}{223734}$ |
| 635 | $\frac{126}{5}$ | 671 | $\frac{58620}{2263}$ |
| 636 | $\frac{3505951}{139020}$ | 672 | $\frac{337}{13}$ |
| 637 | $\frac{1419278889601}{56233877040}$ | 673 | $\frac{48813492618436}{1881620424023}$ |
| 638 | $\frac{42283}{1674}$ | 674 | $\frac{675}{26}$ |
| 639 | $\frac{24220799}{958160}$ | 675 | $\frac{26}{1}$ |
| 640 | $\frac{1039681}{41097}$ | 677 | $\frac{26}{1}$ |
| 641 | $\frac{36120833468}{1426687145}$ | 678 | $\frac{677}{26}$ |
| 642 | $\frac{5777}{228}$ | 679 | $\frac{17792635820}{682818391}$ |
| 643 | $\frac{1988960193026}{78436933185}$ | 680 | $\frac{339}{13}$ |
| 644 | $\frac{11775}{464}$ | 681 | $\frac{10743166003415}{411679015748}$ |
| 645 | $\frac{1024001}{40320}$ | 682 | $\frac{1197901}{45870}$ |
| 646 | $\frac{305}{12}$ | 683 | $\frac{170067682}{6507419}$ |
| 647 | $\frac{120187368}{4725053}$ | 684 | $\frac{57799}{2210}$ |
| 648 | $\frac{19601}{770}$ | 685 | $\frac{218623878}{8353189}$ |
| 649 | $\frac{1123593226162199}{44104892095380}$ | 686 | $\frac{10850138895}{414260228}$ |
| 650 | $\frac{51}{2}$ | 687 | $\frac{165337}{6308}$ |
| 651 | $\frac{1735}{68}$ | 688 | $\frac{24248647}{924471}$ |
| 652 | $\frac{8212499464391371}{321626301397510}$ | 689 | $\frac{105}{4}$ |
| 653 | $\frac{2291286582}{89664965}$ | 690 | $\frac{1471}{56}$ |
| 654 | $\frac{8915765}{348634}$ | 691 | $\frac{31138100617500578690}{1184549173291609383}$ |
| 655 | $\frac{6543193209}{255228884}$ | 692 | $\frac{2499849}{95030}$ |
| 656 | $\frac{2049}{80}$ | 693 | $\frac{246401}{9360}$ |
| 657 | $\frac{2281249}{89000}$ | 694 | $\frac{6601391379037464238955}{19306[illegible]4160683[illegible]97673114}$ |

## TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|
| 695 | $\frac{33639}{1276}$ | 732 | $\frac{487}{18}$ |
| 696 | $\frac{1451}{55}$ | 733 | $\frac{9882}{365}$ |
| 697 | $\frac{132}{5}$ | 734 | $\frac{10394175}{383656}$ |
| 698 | $\frac{5099}{193}$ | 735 | $\frac{244}{9}$ |
| 699 | $\frac{2271050}{85899}$ | 736 | $\frac{24335}{897}$ |
| 700 | $\frac{8193151}{309672}$ | 737 | $\frac{252971383}{9318468}$ |
| 701 | $\frac{11782}{445}$ | 738 | $\frac{163}{6}$ |
| 702 | $\frac{53}{2}$ | 739 | $\frac{98015661073616742153890}{3605564376516452758671}$ |
| 703 | $\frac{1159172}{43719}$ | 740 | $\frac{9249}{340}$ |
| 704 | $\frac{79201}{2985}$ | 741 | $\frac{7352695}{270108}$ |
| 705 | $\frac{237161}{8932}$ | 742 | $\frac{263091151}{9658380}$ |
| 706 | $\frac{34595}{1302}$ | 743 | $\frac{714024}{26195}$ |
| 707 | $\frac{2526}{95}$ | 744 | $\frac{7501}{275}$ |
| 708 | $\frac{62423}{2346}$ | 745 | $\frac{12769001}{467820}$ |
| 709 | $\frac{18245310}{685217}$ | 746 | $\frac{5534543}{202645}$ |
| 710 | $\frac{1279}{48}$ | 747 | $\frac{82}{3}$ |
| 711 | $\frac{80}{3}$ | 748 | $\frac{5658247}{206886}$ |
| 712 | $\frac{1601}{60}$ | 749 | $\frac{1084616184895}{39631020176}$ |
| 713 | $\frac{5286367}{197976}$ | 750 | $\frac{2550251}{93122}$ |
| 714 | $\frac{4115}{154}$ | 751 | $\frac{7293318466794882424418960}{266136970677206024456793}$ |
| 715 | $\frac{75646}{2829}$ | 752 | $\frac{4607}{168}$ |
| 716 | $\frac{35115719688199}{1312336060110}$ | 753 | $\frac{3085126027863}{112433313484}$ |
| 717 | $\frac{6995399}{261260}$ | 754 | $\frac{20457}{745}$ |
| 718 | $\frac{8933399174036079503}{333391476474140716}$ | 755 | $\frac{1209}{44}$ |
| 719 | $\frac{403480310400}{15047276489}$ | 756 | $\frac{55}{2}$ |
| 720 | $\frac{161}{6}$ | 757 | $\frac{1369326}{49769}$ |
| 721 | $\frac{18632176943892415}{693898530122112}$ | 758 | $\frac{413959717}{15035694}$ |
| 722 | $\frac{275807}{10271}$ | 759 | $\frac{551}{20}$ |
| 723 | $\frac{242}{9}$ | 760 | $\frac{52021}{1887}$ |
| 724 | $\frac{2469645423834185801}{91783649341730970}$ | 761 | $\frac{800}{29}$ |
| 725 | $\frac{9801}{364}$ | 762 | $\frac{6349}{230}$ |
| 726 | $\frac{485}{18}$ | 763 | $\frac{719724601}{26055780}$ |
| 727 | $\frac{728}{27}$ | 764 | $\frac{161784071999999}{58533142302000}$ |
| 728 | $\frac{27}{1}$ | 765 | $\frac{285769}{10332}$ |
| 730 | $\frac{27}{1}$ | 766 | $\frac{145933615941744638015}{52727957288616238\text{[illegible]}}$ |
| 731 | $\frac{730}{27}$ | 767 | $\frac{32875}{1187}$ |

# TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|
| 768 | $\frac{18817}{679}$ | 805 | $\frac{1514868641}{53392104}$ |
| 769 | $\frac{16367574077549140}{590322604844777}$ | 806 | $\frac{6196595}{217302}$ |
| 770 | $\frac{111}{4}$ | 807 | $\frac{51841948}{1824925}$ |
| 771 | $\frac{1000081550}{167548057}$ | 808 | $\frac{19731763}{694161}$ |
| 772 | $\frac{6224323426849}{224018302020}$ | 809 | $\frac{422036886190}{14838147833}$ |
| 773 | $\frac{1343018}{48305}$ | 810 | $\frac{27379}{962}$ |
| 774 | $\frac{10405}{374}$ | 811 | $\frac{13832072161578616410}{4853111176233928197}$ |
| 775 | $\frac{4620799}{165984}$ | 812 | $\frac{57}{2}$ |
| 776 | $\frac{195}{7}$ | 813 | $\frac{2167}{76}$ |
| 777 | $\frac{223}{8}$ | 814 | $\frac{4206992174549}{147454139410}$ |
| 778 | $\frac{54610269}{1957873}$ | 815 | $\frac{156644}{5487}$ |
| 779 | $\frac{11785490}{422259}$ | 816 | $\frac{4999}{175}$ |
| 780 | $\frac{391}{14}$ | 817 | $\frac{343}{12}$ |
| 781 | $\frac{67606199}{2419140}$ | 818 | $\frac{143}{5}$ |
| 782 | $\frac{783}{28}$ | 819 | $\frac{1574}{55}$ |
| 783 | $\frac{28}{1}$ | 820 | $\frac{39689}{1386}$ |
| 785 | $\frac{28}{1}$ | 821 | $\frac{2121436703918}{74058651461}$ |
| 786 | $\frac{785}{28}$ | 822 | $\frac{7397}{258}$ |
| 787 | $\frac{34625394240}{1234262007}$ | 823 | $\frac{935170474905644006168}{81975327430497656651}$ |
| 788 | $\frac{393}{14}$ | 824 | $\frac{59535}{2074}$ |
| 789 | $\frac{16116667272575}{573768548496}$ | 825 | $\frac{48599}{1692}$ |
| 790 | $\frac{6616066879}{235389096}$ | 826 | $\frac{222259504685}{7733694382}$ |
| 791 | $\frac{225}{8}$ | 827 | $\frac{900602}{31317}$ |
| 792 | $\frac{197}{7}$ | 828 | $\frac{1151}{40}$ |
| 793 | $\frac{4393}{156}$ | 829 | $\frac{15489282}{537965}$ |
| 794 | $\frac{30235}{1073}$ | 830 | $\frac{146411}{5082}$ |
| 795 | $\frac{6626}{235}$ | 831 | $\frac{9799705}{339948}$ |
| 796 | $\frac{529178298454520220799}{18756227493635015480}$ | 832 | $\frac{842401}{29205}$ |
| 797 | $\frac{24715982}{875485}$ | 833 | $\frac{9478647}{328416}$ |
| 798 | $\frac{113}{4}$ | 834 | $\frac{6552578705}{226897344}$ |
| 799 | $\frac{424}{15}$ | 835 | $\frac{34336355806}{1188258591}$ |
| 800 | $\frac{19601}{693}$ | 836 | $\frac{46551}{1610}$ |
| 801 | $\frac{5000200001}{176670200}$ | 837 | $\frac{12151}{420}$ |
| 802 | $\frac{295496099}{10434330}$ | 838 | $\frac{42112785797}{1454763046}$ |
| 803 | $\frac{7226}{255}$ | 839 | $\frac{840}{29}$ |
| 804 | $\frac{515095}{18166}$ | 840 | $\frac{29}{1}$ |

# TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|
| 842 | $\frac{29}{1}$ | 878 | $\frac{9308601}{314150}$ |
| 843 | $\frac{842}{29}$ | 879 | $\frac{1072451374}{36172395}$ |
| 844 | $\frac{154962314660167628644999}{5334022845973817143410}$ | 880 | $\frac{89}{3}$ |
| 845 | $\frac{12238}{421}$ | 881 | $\frac{106316171438}{3581862825}$ |
| 846 | $\frac{2143295}{73686}$ | 882 | $\frac{19601}{660}$ |
| 847 | $\frac{8193151}{281520}$ | 883 | $\frac{34878175759617272473442}{1173754162936357802169}$ |
| 848 | $\frac{66249}{2275}$ | 884 | $\frac{1665}{56}$ |
| 849 | $\frac{15016554719048695}{515366516330476}$ | 885 | $\frac{119}{4}$ |
| 850 | $\frac{2449}{84}$ | 886 | $\frac{774357459105765518551637765}{260148796464024194010338}$ |
| 851 | $\frac{8129989}{278685}$ | 887 | $\frac{469224}{15755}$ |
| 852 | $\frac{194399}{6660}$ | 888 | $\frac{149}{5}$ |
| 853 | $\frac{10379165955018}{355371343743}$ | 889 | $\frac{13251971717803657215}{4437861554134133504}$ |
| 854 | $\frac{1294299}{44290}$ | 890 | $\frac{179}{6}$ |
| 855 | $\frac{3041}{104}$ | 891 | $\frac{3970}{133}$ |
| 856 | $\frac{6953715867665}{23767172838}$ | 892 | $\frac{100351}{3360}$ |
| 857 | $\frac{8118568}{277325}$ | 893 | $\frac{6091464999}{203843100}$ |
| 858 | $\frac{703}{24}$ | 894 | $\frac{299}{10}$ |
| 859 | $\frac{2058844771979643060124010}{70246877103594937291267}$ | 895 | $\frac{359}{12}$ |
| 860 | $\frac{3871}{132}$ | 896 | $\frac{449}{15}$ |
| 861 | $\frac{541601801}{18457740}$ | 897 | $\frac{599}{20}$ |
| 862 | $\frac{3580225661473121225505}{121942969974921665128}$ | 898 | $\frac{899}{30}$ |
| 863 | $\frac{18534096608}{630905199}$ | 899 | $\frac{30}{1}$ |
| 864 | $\frac{470449}{16005}$ | 901 | $\frac{30}{1}$ |
| 865 | $\frac{3588145108}{121844089}$ | 902 | $\frac{901}{30}$ |
| 866 | $\frac{42435}{1442}$ | 903 | $\frac{601}{20}$ |
| 867 | $\frac{70226}{2385}$ | 904 | $\frac{451}{15}$ |
| 868 | $\frac{3844063}{130476}$ | 905 | $\frac{361}{12}$ |
| 869 | $\frac{601923738698751}{20418948807200}$ | 906 | $\frac{301}{10}$ |
| 870 | $\frac{59}{2}$ | 907 | $\frac{123823410341073497682}{4111458857741309517}$ |
| 871 | $\frac{26351782210}{892896077}$ | 908 | $\frac{102151}{3390}$ |
| 872 | $\frac{126003}{4267}$ | 909 | $\frac{80801}{2680}$ |
| 873 | $\frac{62809633}{2125784}$ | 910 | $\frac{181}{6}$ |
| 874 | $\frac{3725}{126}$ | 911 | $\frac{3718332184927520}{12319363142913}$ |
| 875 | $\frac{120126}{4061}$ | 912 | $\frac{151}{5}$ |
| 876 | $\frac{10951}{370}$ | 913 | $\frac{5157342430820407}{170683122513564}$ |
| 877 | $\frac{241326}{8149}$ | 914 | $\frac{5593}{185}$ |

| N. | FRACTIONS. |
|---|---|
| 915 | $\frac{121}{4}$ |
| 916 | $\frac{5848201}{193230}$ |
| 917 | $\frac{823604599}{27197820}$ |
| 918 | $\frac{4120901}{136010}$ |
| 919 | $\frac{4481603010937119451551263720}{147834442396336739781499369}$ |
| 920 | $\frac{91}{3}$ |
| 921 | $\frac{25220577128835735}{831046527139412}$ |
| 922 | $\frac{4149288307}{136649583}$ |
| 923 | $\frac{638}{21}$ |
| 924 | $\frac{11551}{380}$ |
| 925 | $\frac{882}{29}$ |
| 926 | $\frac{3045560297142335}{100083472361032}$ |
| 927 | $\frac{227528}{7473}$ |
| 928 | $\frac{768555217}{25229031}$ |
| 929 | $\frac{81317086468}{2667927065}$ |
| 930 | $\frac{61}{2}$ |
| 931 | $\frac{6681448801}{218975640}$ |
| 932 | $\frac{10072400673}{329937612}$ |
| 933 | $\frac{75263}{2464}$ |
| 934 | $\frac{3034565}{99294}$ |
| 935 | $\frac{1376}{45}$ |
| 936 | $\frac{5201}{170}$ |
| 937 | $\frac{4902266951010796}{160150080532621}$ |
| 938 | $\frac{17151}{560}$ |
| 939 | $\frac{122695}{4004}$ |
| 940 | $\frac{4231}{138}$ |
| 941 | $\frac{731069390}{23832181}$ |
| 942 | $\frac{106133}{3458}$ |
| 943 | $\frac{737}{24}$ |
| 944 | $\frac{561801}{18285}$ |
| 945 | $\frac{275561}{8964}$ |
| 946 | $\frac{45225786400145}{1470417148788}$ |
| 947 | $\frac{13509645362}{439004487}$ |
| 948 | $\frac{228151}{7410}$ |
| 949 | $\frac{17458841558590}{566738044393}$ |
| 950 | $\frac{202501}{6570}$ |
| 951 | $\frac{224208076}{7270443}$ |
| 952 | $\frac{11663}{378}$ |
| 953 | $\frac{2746864744}{88979577}$ |
| 954 | $\frac{320800351}{10386310}$ |
| 955 | $\frac{2090916349}{67660900}$ |
| 956 | $\frac{78719023628799}{2545964143480}$ |
| 957 | $\frac{14849}{480}$ |
| 958 | $\frac{46761522330425599}{1510772314048580}$ |
| 959 | $\frac{960}{31}$ |
| 960 | $\frac{31}{1}$ |
| 962 | $\frac{31}{1}$ |
| 963 | $\frac{962}{31}$ |
| 964 | $\frac{10085143557001249}{324820603322300}$ |
| 965 | $\frac{14911}{480}$ |
| 966 | $\frac{57499}{1850}$ |
| 967 | $\frac{4649532557817485538}{149518887194649693}$ |
| 968 | $\frac{19601}{630}$ |
| 969 | $\frac{13588951}{436540}$ |
| 970 | $\frac{328173}{10537}$ |
| 971 | $\frac{12479806786330}{400496058813}$ |
| 972 | $\frac{9863382131}{316368130}$ |
| 973 | $\frac{903223}{28956}$ |
| 974 | $\frac{4888215745335215}{15662987165124}$ |
| 975 | $\frac{1249}{40}$ |
| 976 | $\frac{1766319049}{56538495}$ |
| 977 | $\frac{2376748868}{76039103}$ |
| 978 | $\frac{118337}{3784}$ |
| 979 | $\frac{360449}{11520}$ |
| 980 | $\frac{51841}{1656}$ |
| 981 | $\frac{158070671986249}{5046808151760}$ |
| 982 | $\frac{8837}{282}$ |
| 983 | $\frac{284088}{9061}$ |
| 984 | $\frac{88805}{2831}$ |
| 985 | $\frac{408}{13}$ |
| 986 | $\frac{157}{5}$ |
| 987 | $\frac{377}{12}$ |

## TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|
| 988 | $\frac{14549450527}{462879654}$ | 996 | $\frac{8553815}{271038}$ |
| 989 | $\frac{550271588560695}{174976185334396}$ | 997 | $\frac{84906}{2689}$ |
| 990 | $\frac{881}{28}$ | 998 | $\frac{984076901}{31150410}$ |
| 991 | $\frac{379516400906811930638014896080}{12055735790332359447442538767}$ | 999 | $\frac{102688615}{3248924}$ |
| 992 | $\frac{63}{2}$ | 1000 | $\frac{39480499}{1248483}$ |
| 993 | $\frac{2647}{84}$ | 1001 | $\frac{1010905}{31952}$ |
| 994 | $\frac{1135}{36}$ | 1002 | $\frac{2068692247}{65352448}$ |
| 995 | $\frac{8835999}{280120}$ | 1003 | $\frac{9026}{285}$ |

FIN.

A PARIS, DE L'IMPRIMERIE DE CRAPELET.





TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|---|---|
| 364 | $\frac{4954951}{259710}$ | 401 | $\frac{20}{1}$ | 437 | $\frac{4599}{220}$ |
| 365 | $\frac{3458}{181}$ | 402 | $\frac{401}{20}$ | 438 | $\frac{293}{14}$ |
| 366 | $\frac{907925}{47458}$ | 403 | $\frac{669878}{33369}$ | 439 | $\frac{440}{21}$ |
| 367 | $\frac{19019993568}{992833687}$ | 404 | $\frac{201}{10}$ | 440 | $\frac{21}{1}$ |
| 368 | $\frac{1151}{60}$ | 405 | $\frac{161}{8}$ | 442 | $\frac{21}{1}$ |
| 369 | $\frac{8396801}{437120}$ | 406 | $\frac{59468095}{2951352}$ | 443 | $\frac{442}{21}$ |
| 370 | $\frac{327}{17}$ | 407 | $\frac{2663}{132}$ | 444 | $\frac{295}{14}$ |
| 371 | $\frac{1695}{88}$ | 408 | $\frac{101}{5}$ | 445 | $\frac{4662}{221}$ |
| 372 | $\frac{12151}{630}$ | 409 | $\frac{1119221796968}{55341766851}$ | 446 | $\frac{1101660115}{52165112}$ |
| 373 | $\frac{5118}{265}$ | 410 | $\frac{81}{4}$ | 447 | $\frac{148}{7}$ |
| 374 | $\frac{3365}{174}$ | 411 | $\frac{49730}{2453}$ | 448 | $\frac{127}{6}$ |
| 375 | $\frac{15124}{781}$ | 412 | $\frac{103537981367}{5100930235}$ | 449 | $\frac{189471332}{8941705}$ |
| 376 | $\frac{2143295}{110532}$ | 413 | $\frac{113399}{5580}$ | 450 | $\frac{19601}{924}$ |
| 377 | $\frac{233}{12}$ | 414 | $\frac{24335}{1196}$ | 451 | $\frac{46471490}{2188217}$ |
| 378 | $\frac{8749}{450}$ | 415 | $\frac{18412804}{903849}$ | 452 | $\frac{1204353}{56648}$ |
| 379 | $\frac{12941197220540690}{664744650125541}$ | 416 | $\frac{5201}{255}$ | 453 | $\frac{1653751}{77700}$ |
| 380 | $\frac{39}{2}$ | 417 | $\frac{85322647}{4178268}$ | 454 | $\frac{16916040084175685}{793909090494766}$ |
| 381 | $\frac{1015}{52}$ | 418 | $\frac{33857}{1656}$ | 455 | $\frac{64}{3}$ |
| 382 | $\frac{164998439999}{8442054600}$ | 419 | $\frac{270174970}{13198911}$ | 456 | $\frac{1025}{48}$ |
| 383 | $\frac{18768}{959}$ | 420 | $\frac{41}{2}$ | 457 | $\frac{59089951584}{2764111349}$ |
| 384 | $\frac{4801}{245}$ | 421 | $\frac{44042445696821418}{2146497463530785}$ | 458 | $\frac{107}{5}$ |
| 385 | $\frac{95831}{4884}$ | 422 | $\frac{7022501}{341850}$ | 459 | $\frac{499850}{23331}$ |
| 386 | $\frac{111555}{5678}$ | 423 | $\frac{4607}{224}$ | 460 | $\frac{2535751}{118230}$ |
| 387 | $\frac{3482}{177}$ | 424 | $\frac{32080051}{1557945}$ | 461 | $\frac{24314110}{1132421}$ |
| 388 | $\frac{62809633}{3188676}$ | 425 | $\frac{268}{13}$ | 462 | $\frac{43}{2}$ |
| 389 | $\frac{1282}{65}$ | 426 | $\frac{88751}{4300}$ | 463 | $\frac{24751227204156768}{1150285916453161}$ |
| 390 | $\frac{79}{4}$ | 427 | $\frac{62}{3}$ | 464 | $\frac{9801}{455}$ |
| 391 | $\frac{7338680}{371133}$ | 428 | $\frac{1850887}{89466}$ | 465 | $\frac{15871}{736}$ |
| 392 | $\frac{99}{5}$ | 429 | $\frac{1524095}{73584}$ | 466 | $\frac{938319425}{43466808}$ |
| 393 | $\frac{46437143}{2342444}$ | 430 | $\frac{2862251}{138030}$ | 467 | $\frac{1625626}{75225}$ |
| 394 | $\frac{395023035}{19900973}$ | 431 | $\frac{151560720}{7300423}$ | 468 | $\frac{649}{30}$ |
| 395 | $\frac{159}{8}$ | 432 | $\frac{1351}{65}$ | 469 | $\frac{137215}{6336}$ |
| 396 | $\frac{199}{10}$ | 433 | $\frac{7230660684}{347483377}$ | 470 | $\frac{1691}{78}$ |
| 397 | $\frac{20863372242}{1047100765}$ | 434 | $\frac{125}{6}$ | 471 | $\frac{7838695}{361188}$ |
| 398 | $\frac{399}{20}$ | 435 | $\frac{146}{7}$ | 472 | $\frac{306917}{14127}$ |
| 399 | $\frac{20}{1}$ | 436 | $\frac{158070671986249}{7570212227550}$ | 473 | $\frac{87}{4}$ |

## TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|
| 474 | $\frac{193549}{8890}$ | 511 | $\frac{4188548960}{185294497}$ |
| 475 | $\frac{57799}{2652}$ | 512 | $\frac{665857}{29427}$ |
| 476 | $\frac{28799}{1320}$ | 513 | $\frac{13771351}{608020}$ |
| 477 | $\frac{8777860001}{401910600}$ | 514 | $\frac{4625}{204}$ |
| 478 | $\frac{1617319577991743}{73974475617896}$ | 515 | $\frac{17406}{767}$ |
| 479 | $\frac{2989440}{136591}$ | 516 | $\frac{16855}{742}$ |
| 480 | $\frac{241}{11}$ | 517 | $\frac{590968985399}{25990786260}$ |
| 481 | $\frac{964140}{43961}$ | 518 | $\frac{2367}{104}$ |
| 482 | $\frac{483}{22}$ | 519 | $\frac{14851876}{651925}$ |
| 483 | $\frac{22}{1}$ | 520 | $\frac{6499}{285}$ |
| 485 | $\frac{22}{1}$ | 521 | $\frac{128377240}{5624309}$ |
| 486 | $\frac{485}{22}$ | 522 | $\frac{19603}{858}$ |
| 487 | $\frac{11906073840568}{03520887322477}$ | 523 | $\frac{81810300626}{3577314673}$ |
| 488 | $\frac{243}{11}$ | 524 | $\frac{225144199}{9835470}$ |
| 489 | $\frac{7592629977}{343350196}$ | 525 | $\frac{6049}{264}$ |
| 490 | $\frac{1039681}{46968}$ | 526 | $\frac{84156091456952923771}{3666119767224284532}$ |
| 491 | $\frac{93628044170}{4225374483}$ | 527 | $\frac{528}{23}$ |
| 492 | $\frac{29767}{1342}$ | 528 | $\frac{23}{1}$ |
| 493 | $\frac{683982}{30805}$ | 530 | $\frac{23}{1}$ |
| 494 | $\frac{71035}{3196}$ | 531 | $\frac{530}{23}$ |
| 495 | $\frac{89}{4}$ | 532 | $\frac{2588599}{112230}$ |
| 496 | $\frac{4620799}{207480}$ | 533 | $\frac{6118}{265}$ |
| 497 | $\frac{1201887}{53910}$ | 534 | $\frac{3678725}{159194}$ |
| 498 | $\frac{179777}{8056}$ | 535 | $\frac{1618804}{69987}$ |
| 499 | $\frac{4490}{201}$ | 536 | $\frac{145925}{6303}$ |
| 500 | $\frac{930249}{41602}$ | 537 | $\frac{192349463}{8300492}$ |
| 501 | $\frac{11242731902975}{502258218432}$ | 538 | $\frac{69051}{2977}$ |
| 502 | $\frac{3832352837}{171046278}$ | 539 | $\frac{3970}{171}$ |
| 503 | $\frac{24648}{1099}$ | 540 | $\frac{119071}{5124}$ |
| 504 | $\frac{449}{20}$ | 541 | $\frac{1361516316459227452}{58536158470221581}$ |
| 505 | $\frac{809}{36}$ | 542 | $\frac{4293183}{184408}$ |
| 506 | $\frac{45}{2}$ | 543 | $\frac{669337}{28724}$ |
| 507 | $\frac{1351}{60}$ | 544 | $\frac{2449}{105}$ |
| 508 | $\frac{44757606858751}{1985797689600}$ | 545 | $\frac{1961}{84}$ |
| 509 | $\frac{395727950}{17540333}$ | 546 | $\frac{701}{30}$ |
| 510 | $\frac{271}{12}$ | 547 | $\frac{160177601264642}{6848699678673}$ |

| N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|
| 548 | $\frac{5083073}{219856}$ | 585 | $\frac{33281}{1376}$ |
| 549 | $\frac{1766319049}{75384660}$ | 586 | $\frac{4115086707}{169992665}$ |
| 550 | $\frac{30580901}{1303974}$ | 587 | $\frac{1907162}{78717}$ |
| 551 | $\frac{8380}{357}$ | 588 | $\frac{97}{4}$ |
| 552 | $\frac{47}{2}$ | 589 | $\frac{41423166067036213711}{1706811823063746000}$ |
| 553 | $\frac{624635837407}{26562217704}$ | 590 | $\frac{5781}{238}$ |
| 554 | $\frac{174293}{7405}$ | 591 | $\frac{165676}{6815}$ |
| 555 | $\frac{1814}{77}$ | 592 | $\frac{73}{3}$ |
| 556 | $\frac{12032115501124999}{510273338434250}$ | 593 | $\frac{600630}{24665}$ |
| 557 | $\frac{118}{5}$ | 594 | $\frac{1098305}{45064}$ |
| 558 | $\frac{7937}{336}$ | 595 | $\frac{18514}{759}$ |
| 559 | $\frac{506568295}{21425516}$ | 596 | $\frac{25801741449}{1056880510}$ |
| 560 | $\frac{71}{3}$ | 597 | $\frac{463287093751}{18961078500}$ |
| 561 | $\frac{522785}{22072}$ | 598 | $\frac{1574351}{64380}$ |
| 562 | $\frac{220938497}{9319728}$ | 599 | $\frac{24686379794520}{1008658133851}$ |
| 563 | $\frac{68122}{2871}$ | 600 | $\frac{49}{2}$ |
| 564 | $\frac{95}{4}$ | 601 | $\frac{139468303679530}{5689030769845}$ |
| 565 | $\frac{147312278}{620633}$ | 602 | $\frac{687}{28}$ |
| 566 | $\frac{95609283}{4018718}$ | 603 | $\frac{48842}{1989}$ |
| 567 | $\frac{2024}{85}$ | 604 | $\frac{5972991296311683199}{243037369063951720}$ |
| 568 | $\frac{143}{6}$ | 605 | $\frac{930249}{37820}$ |
| 569 | $\frac{2894863830}{121359005}$ | 606 | $\frac{42187499}{1713710}$ |
| 570 | $\frac{191}{8}$ | 607 | $\frac{164076033968}{6659640783}$ |
| 571 | $\frac{181124553061630786130}{7379818350628982587}$ | 608 | $\frac{2737}{111}$ |
| 572 | $\frac{287}{12}$ | 609 | $\frac{601695}{24344}$ |
| 573 | $\frac{383}{16}$ | 610 | $\frac{71847}{2909}$ |
| 574 | $\frac{575}{24}$ | 611 | $\frac{236926}{9585}$ |
| 575 | $\frac{24}{1}$ | 612 | $\frac{2177}{88}$ |
| 577 | $\frac{24}{1}$ | 613 | $\frac{482173579088618}{19414619624065}$ |
| 578 | $\frac{577}{24}$ | 614 | $\frac{348291186245}{14055888314}$ |
| 579 | $\frac{385}{16}$ | 615 | $\frac{124}{5}$ |
| 580 | $\frac{289}{12}$ | 616 | $\frac{21295}{858}$ |
| 581 | $\frac{152071153971}{6308974348}$ | 617 | $\frac{41009716}{1650989}$ |
| 582 | $\frac{193}{8}$ | 618 | $\frac{10093}{406}$ |
| 583 | $\frac{8429143}{349116}$ | 619 | $\frac{5172113654388408730}{207885569071159439}$ |
| 584 | $\frac{145}{6}$ | 620 | $\frac{249}{10}$ |

# TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|
| 621 | $\frac{7775}{312}$ | 658 | $\frac{1693}{66}$ |
| 622 | $\frac{138043770061}{5535048010}$ | 659 | $\frac{5930}{231}$ |
| 623 | $\frac{624}{25}$ | 660 | $\frac{1079}{42}$ |
| 624 | $\frac{25}{1}$ | 661 | $\frac{28654544754245933218}{1114513260249634695}$ |
| 626 | $\frac{25}{1}$ | 662 | $\frac{1718102101}{66773950}$ |
| 627 | $\frac{626}{25}$ | 663 | $\frac{103}{4}$ |
| 628 | $\frac{466987287311849}{1863482146110}$ | 664 | $\frac{1700902565}{66007621}$ |
| 629 | $\frac{8100}{323}$ | 665 | $\frac{13719}{532}$ |
| 630 | $\frac{251}{10}$ | 666 | $\frac{27361201}{1060380}$ |
| 631 | $\frac{48961575312998650035560}{1949129537575151036427}$ | 667 | $\frac{1071119047}{41476668}$ |
| 632 | $\frac{7743}{308}$ | 668 | $\frac{56447}{2184}$ |
| 633 | $\frac{440772247}{17519124}$ | 669 | $\frac{14226117859054131}{550018492618436}$ |
| 634 | $\frac{65999458125}{2621173333}$ | 670 | $\frac{5791211}{223734}$ |
| 635 | $\frac{126}{5}$ | 671 | $\frac{58620}{2263}$ |
| 636 | $\frac{3105951}{123160}$ | 672 | $\frac{337}{13}$ |
| 637 | $\frac{1419278889601}{56233877040}$ | 673 | $\frac{48817492618436}{1881620424025}$ |
| 638 | $\frac{42283}{1674}$ | 674 | $\frac{675}{26}$ |
| 639 | $\frac{24220799}{958160}$ | 675 | $\frac{26}{1}$ |
| 640 | $\frac{1039681}{41097}$ | 677 | $\frac{26}{1}$ |
| 641 | $\frac{36120833468}{1426687145}$ | 678 | $\frac{677}{26}$ |
| 642 | $\frac{5777}{228}$ | 679 | $\frac{1779261555320}{68281182391}$ |
| 643 | $\frac{1988960193026}{784169331185}$ | 680 | $\frac{339}{13}$ |
| 644 | $\frac{11775}{464}$ | 681 | $\frac{10743166003415}{411679015748}$ |
| 645 | $\frac{1024001}{40320}$ | 682 | $\frac{1197901}{45870}$ |
| 646 | $\frac{305}{12}$ | 683 | $\frac{170067682}{6507419}$ |
| 647 | $\frac{120188168}{4725013}$ | 684 | $\frac{57799}{2210}$ |
| 648 | $\frac{19601}{770}$ | 685 | $\frac{218623878}{8353189}$ |
| 649 | $\frac{112311973226162199}{4410489209538 0}$ | 686 | $\frac{10850138891}{414260228}$ |
| 650 | $\frac{51}{2}$ | 687 | $\frac{165337}{6308}$ |
| 651 | $\frac{1735}{68}$ | 688 | $\frac{24248647}{924470}$ |
| 652 | $\frac{8213499464321351}{321626301297510}$ | 689 | $\frac{105}{4}$ |
| 653 | $\frac{2291286382}{89664965}$ | 690 | $\frac{1471}{56}$ |
| 654 | $\frac{8911761}{348634}$ | 691 | $\frac{31138100617500578690}{1184549178291009381}$ |
| 655 | $\frac{654319209}{25528884}$ | 692 | $\frac{2499849}{95030}$ |
| 656 | $\frac{2049}{80}$ | 693 | $\frac{246401}{9360}$ |
| 657 | $\frac{2281249}{89000}$ | 694 | $\frac{66013912790374642382785}{1980674060683976722114}$ |

| N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|
| 695 | $\frac{33639}{1276}$ | 732 | $\frac{487}{18}$ |
| 696 | $\frac{1451}{55}$ | 733 | $\frac{9882}{365}$ |
| 697 | $\frac{132}{5}$ | 734 | $\frac{10394175}{383656}$ |
| 698 | $\frac{5099}{193}$ | 735 | $\frac{244}{9}$ |
| 699 | $\frac{2271050}{85899}$ | 736 | $\frac{24335}{897}$ |
| 700 | $\frac{8193151}{309672}$ | 737 | $\frac{252975383}{9318468}$ |
| 701 | $\frac{11732}{443}$ | 738 | $\frac{163}{6}$ |
| 702 | $\frac{53}{2}$ | 739 | $\frac{98015661073616742133890}{3605364376511645273867}$ |
| 703 | $\frac{1159172}{43719}$ | 740 | $\frac{9249}{340}$ |
| 704 | $\frac{79201}{2985}$ | 741 | $\frac{7352695}{270108}$ |
| 705 | $\frac{237161}{8932}$ | 742 | $\frac{263091151}{9658380}$ |
| 706 | $\frac{34595}{1302}$ | 743 | $\frac{714024}{26195}$ |
| 707 | $\frac{2526}{95}$ | 744 | $\frac{7501}{275}$ |
| 708 | $\frac{62423}{2346}$ | 745 | $\frac{12769001}{467820}$ |
| 709 | $\frac{18245310}{685217}$ | 746 | $\frac{5534843}{202643}$ |
| 710 | $\frac{1279}{48}$ | 747 | $\frac{82}{3}$ |
| 711 | $\frac{80}{3}$ | 748 | $\frac{5658247}{206886}$ |
| 712 | $\frac{1601}{60}$ | 749 | $\frac{1084616384895}{39631020176}$ |
| 713 | $\frac{5286367}{197976}$ | 750 | $\frac{2550251}{93122}$ |
| 714 | $\frac{4115}{154}$ | 751 | $\frac{7293318466794882424418960}{266136970677206024456793}$ |
| 715 | $\frac{75646}{2829}$ | 752 | $\frac{4607}{168}$ |
| 716 | $\frac{35115719688199}{1312336060110}$ | 753 | $\frac{3085126027863}{112433313484}$ |
| 717 | $\frac{6998399}{261360}$ | 754 | $\frac{20457}{745}$ |
| 718 | $\frac{8933399174056079303}{333391496474140716}$ | 755 | $\frac{1209}{44}$ |
| 719 | $\frac{4034808310400}{150472276489}$ | 756 | $\frac{55}{2}$ |
| 720 | $\frac{161}{6}$ | 757 | $\frac{1369326}{49769}$ |
| 721 | $\frac{186321769432924 15}{6935981301221112}$ | 758 | $\frac{415959717}{15108694}$ |
| 722 | $\frac{275807}{10275}$ | 759 | $\frac{551}{20}$ |
| 723 | $\frac{242}{9}$ | 760 | $\frac{52021}{1887}$ |
| 724 | $\frac{2469641423824185801}{91783649341730979}$ | 761 | $\frac{800}{29}$ |
| 725 | $\frac{9801}{364}$ | 762 | $\frac{6349}{230}$ |
| 726 | $\frac{485}{18}$ | 763 | $\frac{719724699}{26055780}$ |
| 727 | $\frac{728}{27}$ | 764 | $\frac{1617840719999999}{58533142302000}$ |
| 728 | $\frac{27}{1}$ | 765 | $\frac{285769}{10332}$ |
| 730 | $\frac{27}{1}$ | 766 | $\frac{2415933611941744638015}{87287937288636232808}$ |
| 731 | $\frac{730}{27}$ | 767 | $\frac{31212}{1127}$ |

TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|
| 768 | 18817/679 | 805 | 4414368641/155592104 |
| 769 | 16367374077549540/590222604344777 | 806 | 6166395/217202 |
| 770 | 111/4 | 807 | 55841948/1965723 |
| 771 | 4660081530/167848037 | 808 | 19731763/694161 |
| 772 | 6224323426849/224018302020 | 809 | 4220368886190/148547893333 |
| 773 | 1315018/47305 | 810 | 27379/962 |
| 774 | 10405/374 | 811 | 13820721635578516410/485351117623372197 |
| 775 | 4620799/165984 | 812 | 57/2 |
| 776 | 195/7 | 813 | 2167/76 |
| 777 | 223/8 | 814 | 4206992174549/147454999410 |
| 778 | 54610269/1957873 | 815 | 156644/5487 |
| 779 | 11785490/422259 | 816 | 4999/175 |
| 780 | 391/14 | 817 | 343/12 |
| 781 | 67606199/2419140 | 818 | 143/5 |
| 782 | 783/28 | 819 | 1574/55 |
| 783 | 28/1 | 820 | 39689/1386 |
| 785 | 28/1 | 821 | 2121456703918/74058651465 |
| 786 | 785/28 | 822 | 7397/258 |
| 787 | 346255942442/12342632007 | 823 | 8551170474903644006168/81975127434497636051 |
| 788 | 393/14 | 824 | 59535/2074 |
| 789 | 161166667272571/5737685548496 | 825 | 48599/1692 |
| 790 | 66160666879/2353890896 | 826 | 222239304685/7732694382 |
| 791 | 225/8 | 827 | 900602/31317 |
| 792 | 197/7 | 828 | 1151/40 |
| 793 | 4393/156 | 829 | 15489282/537965 |
| 794 | 30235/1073 | 830 | 146411/5082 |
| 795 | 6626/235 | 831 | 9799705/339948 |
| 796 | 5291782933454520220799/187562274936351053480 | 832 | 841401/29170 |
| 797 | 24715982/875485 | 833 | 9478647/328416 |
| 798 | 113/4 | 834 | 6552578705/226897244 |
| 799 | 424/15 | 835 | 34336255806/1188258591 |
| 800 | 19601/693 | 836 | 46551/1610 |
| 801 | 5000200001/176670200 | 837 | 12151/420 |
| 802 | 295496099/10434330 | 838 | 42112785797/1454762046 |
| 803 | 7226/255 | 839 | 840/29 |
| 804 | 515095/18166 | 840 | 29/1 |

# TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|
| 842 | $\frac{29}{1}$ | 878 | $\frac{9308501}{314150}$ |
| 843 | $\frac{842}{29}$ | 879 | $\frac{1072455324}{36172951}$ |
| 844 | $\frac{1549625314660167628644999}{533402285459738171485450}$ | 880 | $\frac{89}{3}$ |
| 845 | $\frac{12238}{421}$ | 881 | $\frac{1063116271412}{3581662831}$ |
| 846 | $\frac{2143295}{73688}$ | 882 | $\frac{19601}{660}$ |
| 847 | $\frac{8193151}{281520}$ | 883 | $\frac{348784757596172724715442}{1173754162936317802169}$ |
| 848 | $\frac{66249}{2275}$ | 884 | $\frac{1665}{56}$ |
| 849 | $\frac{1501654712948695}{515366516330476}$ | 885 | $\frac{119}{4}$ |
| 850 | $\frac{2449}{84}$ | 886 | $\frac{7743524593057455858637765}{260148796464024194210316}$ |
| 851 | $\frac{8129989}{278685}$ | 887 | $\frac{469224}{15755}$ |
| 852 | $\frac{194399}{6660}$ | 888 | $\frac{149}{5}$ |
| 853 | $\frac{10379165955018}{355371543741}$ | 889 | $\frac{11231974717803657215}{443786168413413504}$ |
| 854 | $\frac{1294299}{44290}$ | 890 | $\frac{179}{6}$ |
| 855 | $\frac{3041}{104}$ | 891 | $\frac{3970}{133}$ |
| 856 | $\frac{6913751867665}{23767172838}$ | 892 | $\frac{100351}{3360}$ |
| 857 | $\frac{8118568}{277325}$ | 893 | $\frac{6091434999}{203843100}$ |
| 858 | $\frac{703}{24}$ | 894 | $\frac{299}{10}$ |
| 859 | $\frac{2058844771979643060114010}{70246677103594937291269}$ | 895 | $\frac{359}{12}$ |
| 860 | $\frac{3871}{132}$ | 896 | $\frac{449}{15}$ |
| 861 | $\frac{541601801}{18457740}$ | 897 | $\frac{599}{20}$ |
| 862 | $\frac{35802251661475121251503}{12194296994921665126}$ | 898 | $\frac{899}{30}$ |
| 863 | $\frac{15524026608}{630565199}$ | 899 | $\frac{30}{1}$ |
| 864 | $\frac{470449}{16005}$ | 901 | $\frac{30}{1}$ |
| 865 | $\frac{338345108}{11544089}$ | 902 | $\frac{901}{30}$ |
| 866 | $\frac{42435}{1442}$ | 903 | $\frac{601}{20}$ |
| 867 | $\frac{70226}{2385}$ | 904 | $\frac{451}{15}$ |
| 868 | $\frac{3844063}{130476}$ | 905 | $\frac{361}{12}$ |
| 869 | $\frac{60192738695751}{2041898807200}$ | 906 | $\frac{301}{10}$ |
| 870 | $\frac{59}{2}$ | 907 | $\frac{123825410343075497682}{4111456857741309517}$ |
| 871 | $\frac{263511782210}{892896077}$ | 908 | $\frac{102151}{3390}$ |
| 872 | $\frac{126003}{4267}$ | 909 | $\frac{80801}{2680}$ |
| 873 | $\frac{62809655}{2125784}$ | 910 | $\frac{181}{6}$ |
| 874 | $\frac{3725}{126}$ | 911 | $\frac{371832184927120}{12319363142913}$ |
| 875 | $\frac{120126}{4061}$ | 912 | $\frac{151}{5}$ |
| 876 | $\frac{10951}{370}$ | 913 | $\frac{1157754245080407}{170663122511364}$ |
| 877 | $\frac{241326}{8149}$ | 914 | $\frac{5593}{185}$ |

# TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|
| 915 | $\frac{121}{4}$ | 951 | $\frac{224205576}{7270441}$ |
| 916 | $\frac{5845201}{193130}$ | 952 | $\frac{11663}{378}$ |
| 917 | $\frac{823604199}{27197540}$ | 953 | $\frac{2746864744}{88979677}$ |
| 918 | $\frac{4120901}{136010}$ | 954 | $\frac{32050051}{1037653}$ |
| 919 | $\frac{4481603010937119451551263720}{147834442396536759781499589}$ | 955 | $\frac{2095256249}{67800700}$ |
| 920 | $\frac{91}{3}$ | 956 | $\frac{767190236285799}{24812564244480}$ |
| 921 | $\frac{2522017712831735}{83104627139413}$ | 957 | $\frac{14849}{480}$ |
| 922 | $\frac{4192258107}{138068323}$ | 958 | $\frac{16762522310425599}{541572514048560}$ |
| 923 | $\frac{638}{21}$ | 959 | $\frac{960}{31}$ |
| 924 | $\frac{11551}{380}$ | 960 | $\frac{31}{1}$ |
| 925 | $\frac{882}{29}$ | 962 | $\frac{31}{1}$ |
| 926 | $\frac{3041602971423315}{100084723610032}$ | 963 | $\frac{962}{31}$ |
| 927 | $\frac{227528}{7473}$ | 964 | $\frac{10085143557001249}{324820603522300}$ |
| 928 | $\frac{7658551217}{251409061}$ | 965 | $\frac{14911}{480}$ |
| 929 | $\frac{81317086468}{2667927065}$ | 966 | $\frac{57199}{1840}$ |
| 930 | $\frac{61}{2}$ | 967 | $\frac{46495321557817481535}{1495118887194649693}$ |
| 931 | $\frac{6681448801}{218975640}$ | 968 | $\frac{19601}{630}$ |
| 932 | $\frac{1072400673}{35127652}$ | 969 | $\frac{13558951}{436140}$ |
| 933 | $\frac{75263}{2464}$ | 970 | $\frac{328173}{10537}$ |
| 934 | $\frac{1034161}{33839}$ | 971 | $\frac{12479806786310}{400496018813}$ |
| 935 | $\frac{1376}{45}$ | 972 | $\frac{9863382151}{316368130}$ |
| 936 | $\frac{5201}{170}$ | 973 | $\frac{903223}{28956}$ |
| 937 | $\frac{490226695010796}{16013008054681}$ | 974 | $\frac{455821745235413}{14662987183124}$ |
| 938 | $\frac{17151}{560}$ | 975 | $\frac{1249}{40}$ |
| 939 | $\frac{122695}{4004}$ | 976 | $\frac{1766319049}{56538495}$ |
| 940 | $\frac{4231}{138}$ | 977 | $\frac{7376748868}{236003103}$ |
| 941 | $\frac{7310049390}{235332181}$ | 978 | $\frac{118337}{3784}$ |
| 942 | $\frac{106151}{3458}$ | 979 | $\frac{360449}{11520}$ |
| 943 | $\frac{737}{24}$ | 980 | $\frac{51841}{1656}$ |
| 944 | $\frac{561601}{18278}$ | 981 | $\frac{158070671986249}{5046808151700}$ |
| 945 | $\frac{275561}{8964}$ | 982 | $\frac{8837}{282}$ |
| 946 | $\frac{4132257886400145}{134350417143756}$ | 983 | $\frac{284088}{9061}$ |
| 947 | $\frac{135096451362}{4390044487}$ | 984 | $\frac{88805}{2831}$ |
| 948 | $\frac{228151}{7410}$ | 985 | $\frac{408}{13}$ |
| 949 | $\frac{17455543555570}{566738044393}$ | 986 | $\frac{157}{5}$ |
| 950 | $\frac{196501}{6370}$ | 987 | $\frac{377}{12}$ |

TABLE XII.

| N. | FRACTIONS. | N. | FRACTIONS. |
|---|---|---|---|
| 988 | $\frac{14549450527}{462879684}$ | 996 | $\frac{8553815}{271038}$ |
| 989 | $\frac{1550271588160695}{17497618554396}$ | 997 | $\frac{84906}{2689}$ |
| 990 | $\frac{881}{28}$ | 998 | $\frac{984076901}{31150410}$ |
| 991 | $\frac{379516400906811930638014896080}{12055735790331359447442538767}$ | 999 | $\frac{102688615}{3248924}$ |
| 992 | $\frac{63}{2}$ | 1000 | $\frac{39480499}{1248483}$ |
| 993 | $\frac{2647}{84}$ | 1001 | $\frac{1050905}{33532}$ |
| 994 | $\frac{1135}{36}$ | 1002 | $\frac{206869247}{6535248}$ |
| 995 | $\frac{8836999}{280120}$ | 1003 | $\frac{9026}{285}$ |

FIN.

A PARIS, DE L'IMPRIMERIE DE CRAPELET.

